

DRAFT

GUIDE TO OSCAL- BASED FEDRAMP SYSTEM SECURITY PLANS

Version 1.0

November 27, 2019



FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
11/27/2019	Initial Publication	1.0	FedRAMP PMO
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to Contact Us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact info@FedRAMP.gov.

For more information about FedRAMP, see <https://FedRAMP.gov>.

TABLE OF CONTENTS

Document Revision History	i
1. Overview	1
1.1. Who Should Use This Document?.....	1
1.2. Basic Terminology	1
1.3. XML and JSON Formats	2
1.4. OSCAL-based FedRAMP SSP Template	2
1.5. XML and JSON Technology Standards	3
1.5.1. NIST OSCAL Syntax Validation Mechanisms	3
1.5.2. NIST OSCAL Format Conversion Mechanisms.....	3
1.6. XPath Queries and References.....	4
2. Working with OSCAL Files	5
2.1. Sequence and Hierarchy Are Important	5
2.2. Multiple Layers of Validation	6
2.3. OSCAL's Minimum File Requirements	7
2.4. Assigning Identifiers.....	10
2.4.1. Uniqueness of Identifiers.....	10
2.5. Handling of OSCAL Data Types.....	11
2.5.1. Date and Time in OSCAL Files	11
2.5.2. Working With href Flags	12
2.5.3. Markup-line and Markup-multiline Fields in OSCAL.....	13
2.5.4. Working with Markup-multiline Content	14
2.5.5. Special Characters in OSCAL	15
2.6. Citations, Attachments and Embedded Content in OSCAL Files.....	15
3. FedRAMP Extensions, Defined Identifiers, and Accepted Values	17
3.1.1. FedRAMP Extensions	17
3.1.2. FedRAMP Defined Identifiers.....	18
3.1.3. OSCAL and FedRAMP Accepted Values	19
4. SSP Template to OSCAL Mapping	20
4.1. SSP Title Page	21
4.2. SSP Prepared By/For	22
4.3. Document Revision History.....	23
4.4. How to Contact Us	23
4.5. System Security Plan Approvals.....	24
4.6. Information System Name, Title, and FedRAMP Identifier	25
4.7. Information System Categorization and FedRAMP Baselines	26
4.8. Information Types.....	27
4.9. Security Objectives Categorization (FIPS 199)	28

4.10. Digital Identity Determination	29
4.11. Information System Owner.....	30
4.12. Authorizing Officials	31
4.13. Other Designated Contacts: Information System Management	32
4.14. Other Designated Contacts: Information System Technical	33
4.15. Assignment of Security Responsibility: ISSO	34
4.16. Assignment of Security Responsibility: AO POC	35
4.17. Information System Operational Status	36
4.18. Cloud Service Models.....	37
4.19. Cloud Deployment Models	38
4.20. Leveraged Authorizations	39
4.21. System Function or Purpose	40
4.22. Authorization Boundary Diagram	41
4.23. Personnel Roles and Privileges	42
4.24. Number of Users	43
4.25. Network Architecture Diagram(s).....	44
4.26. Data Flow Diagrams	45
4.27. Ports, Protocols and Services.....	46
4.28. System Interconnections and Authorized Connections (Representation)	47
4.29. System Interconnections and Authorized Connections (Queries)	48
4.30. Laws, Regulations, Standards and Guidance	49
5. Security Controls	50
5.1. Control Definitions.....	51
5.2. Responsible Roles and Parameter Assignments	52
5.3. Implementation Status	53
5.4. Control Origination	54
5.5. Control Implementation Description: Overview.....	55
5.5.1. Policy and Procedure Statements.....	55
5.5.2. Multi-Part Statements:	55
5.5.3. Single Statement.....	55
5.6. Control Implementation Description: Approaches.....	56
5.6.1. Flat-File Approach	57
5.6.2. Component Approach.....	58
5.6.3. XPath Queries for Control Implementation Descriptions	59
6. Attachments	60
6.1. Attachments.....	61
6.2. Privacy Impact Assessment: POC	62
6.3. Privacy Impact Assessment: Laws and Regulations	63
6.4. Privacy Impact Assessment: Designation and Qualifying Questions	64
6.5. System Inventory Approach.....	65
6.5.1. Flat File Approach	66
6.5.2. Component-based Approach.....	67

6.5.3. Inventory Data Locations and XPath Queries	68
7. Generated Content.....	74
7.1. Generating the Control Information Summary (CIS)	74
7.2. Generating the Customer Responsibility Matrix (CRM)	74
Appendicies.....	75
Appendix A. OSCAL-Based FedRAMP Baselines	75
Appendix B. Modifying a FedRAMP Baseline	77
Appendix C. Working with Roles, People, and Organizations.....	81
Appendix D. Working with Components	82

I. OVERVIEW

I.1. Who Should Use This Document?

This document is intended for technical staff and tool developers implementing solutions for importing, exporting, and manipulating OSCAL-based FedRAMP SSP content.

It provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SSP files. Our goal is to enable your organization to develop tools that will seamlessly ensure these standards are met so your security practitioners can focus on SSP content and accuracy rather than formatting and presentation.

I.2. Basic Terminology

XML and JSON use different terminology. Instead of repeatedly clarifying format-specific terminology, this document uses the following format-agnostic terminology through the document.

TERM	XML EQUIVALENT	JSON EQUIVALENT
Field	A single element or node that can hold a value or an attribute	A single object that can hold a value or property
Flag	Attribute	property
Assembly	A collection of elements or nodes. Typically, a parent node with one or more child nodes.	A collection of objects. Typically, a parent object with one or more child objects.

These terms are used by NIST in the creation of OSCAL syntax.

Throughout this document, the following words are used to differentiate between requirements, recommendations, and options.

TERM	MEANING
must	Indicates a required action.
should	Indicates a recommended action, but not necessarily required.
may	Indicates an optional action.

I.3. XML and JSON Formats

The examples provided here are in XML; however, FedRAMP accepts XML or JSON formatted OSCAL-based SSPs. NIST offers a utility that provides lossless conversion of OSCAL-compliant files between XML and JSON in either direction.

You may submit your SSP to FedRAMP using either format. If necessary, FedRAMP tools will convert the files for processing.

I.4. OSCAL-based FedRAMP SSP Template

FedRAMP offers an OSCAL-based SSP shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that shell file. The OSCAL-based FedRAMP SSP Template is available in XML and JSON formats here:

- OSCAL-based FedRAMP SSP Template (JSON Format):
<https://github.com/GSA/fedramp-automation/raw/master/templates/FedRAMP-SSP-OSCAL-Template.json>
- OSCAL-based FedRAMP SSP Template (XML Format):
<https://github.com/GSA/fedramp-automation/raw/master/templates/FedRAMP-SSP-OSCAL-Template.xml>

I.5. XML and JSON Technology Standards

For OSCAL compliance, mechanisms that interpret or generate OSCAL content must honor the core syntax described at <https://pages.nist.gov/OSCAL/documentation/schema/>.

While not mandatory, organizations adopting OSCAL are strongly encouraged to use the NIST-published validation and translation mechanisms. The validation mechanism ensures XML and JSON files are using OSCAL-compliant syntax, while the translation mechanism converts OSCAL content from either format to the other. NIST has an automated governance process, which ensures these mechanisms remain aligned with the latest OSCAL syntax.

I.5.1. NIST OSCAL Syntax Validation Mechanisms

The NIST OSCAL schema validation files are available here:

XML: <https://github.com/usnistgov/OSCAL/tree/master/xml/schema>
JSON: <https://github.com/usnistgov/OSCAL/tree/master/json/schema>

Validating XML-based OSCAL files using the NIST-published schema validation requires:

XML Schema Definition Language (XSD) 1.1
<https://www.w3.org/TR/xmlschema11-1/>

Validating JSON-based OSCAL files using the NIST-published schema validation requires:

JSON Schema, draft-07
<https://json-schema.org/>

There are several open-source and commercial tools that will process XSD 1.1 or JSON Schema, draft-07, either as stand-alone capabilities or as programming libraries.

FedRAMP and NIST are unable to endorse specific products.

I.5.2. NIST OSCAL Format Conversion Mechanisms

The NIST OSCAL format conversion files are available here:

XML to JSON: <https://github.com/usnistgov/OSCAL/tree/master/json/convert>
JSON to XML: <https://github.com/usnistgov/OSCAL/tree/master/xml/convert>

Converting between XML and JSON in either direction using the NIST built the XML conversion files requires:

Extensible Stylesheet Language Transformation (XSLT) 3.0
<https://www.w3.org/TR/2017/REC-xslt-30-20170608/>

and:

XPath 3.1
<https://www.w3.org/TR/xpath-31/>

There are several open-source and commercial tools that will process XSLT3.0 and XPath 3.1, either as stand-alone capabilities or as programming libraries.

FedRAMP and NIST are unable to endorse specific products.

I.6. XPath Queries and References

Except where noted, all XPath queries in this document are based on XPath 2.0.

Most modern programming languages make XPath 1.0 available by default. XPath 2.0 can typically be added with third-party libraries, or calls to external command-line utilities.

The XPath queries *in this document* have been designed to easily convert from XPath 2.0 to 1.0 using a function similar to the one below, which enables developers to use native XML capabilities.

Sample PHP Code to Prepend Namespace (Converts most XPath 2.0 to 1.0)

```
// $query is the XPath 2.0 query
// $ns is the namespace value which much be prepended to element
//      names in the query
// RETURNS: An XPath 1.0 query
function AddNamespace2xpath($query, $ns) {
    $result = "";
    $q_len = strlen($query);
    $prev_char = "";

    for($i=0; $i < $q_len ; $i++) {
        $cur_char = substr($query, $i, 1);
        if ($prev_char === '/') {
            if (ctype_alpha($cur_char)) {
                $result .= $ns . ":";

            }
        }
        $result .= $cur_char;
        $prev_char = $cur_char;
    }

    return $result;
}
```

Even if you do not use XPath to query the data file, the XPath queries provide a concise and non-ambiguous way to communicate where the data is within the file.

Most XPath queries in this document are absolute paths from the root of the document. In other words, it is clear from the XPath query which of the major file sections described in Section 2.3 is being referenced, and where the field is located within the section.

JSON Users: There are several JSON query technologies available, such as JSONPath [<https://restfulapi.net/json-jsonpath/>]; however, no one technology has emerged as a clear standard as of this publication.

Database Users: Some tool developers prefer to manage OSCAL data by first importing it into a database. This is an acceptable approach, provided any resulting OSCAL file generated from the database follows the OSCAL syntax. If the file is intended for delivery to FedRAMP, it must also follow the guidance in this document.

There are also database-like XML servers, such as the open-source tool BaseX [<http://www.basex.org/>], which allow OSCAL files to remain in their native format, yet be queried more like a traditional database. The queries are also optimized for performance.

2. WORKING WITH OSCAL FILES

This section covers several important concepts and details that apply to OSCAL-based FedRAMP SSP files.

2.1. Sequence and Hierarchy Are Important

At any given level, the syntax validation rules for XML-based OSCAL files requires the fields and assemblies to appear in a particular order. Further, the hierarchy of field placement within assemblies is important. The same field name is interpreted differently in different assemblies. For example, the `title` field under metadata is the document title, while the `title` field under role gives a human-friendly name to that role.

XML-based OSCAL files fail the basic NIST validation if this is not honored. Fortunately, NIST's documentation presents the fields and assemblies in the correct sequence.

Always use the sequence found here:

<https://pages.nist.gov/OSCAL/documentation/schema/ssp/xml-model-map/>

Most XML assemblies in OSCAL follow a general sequence as follows:

- <title> field
- <description> field
- <prop> fields
- <annotation> assemblies
- assembly-specific fields
- <remarks> field

Not all of the above are present in every assembly. Any that are present follow this pattern.

2.2. Multiple Layers of Validation

There are several layers at which an OSCAL file can be considered valid.

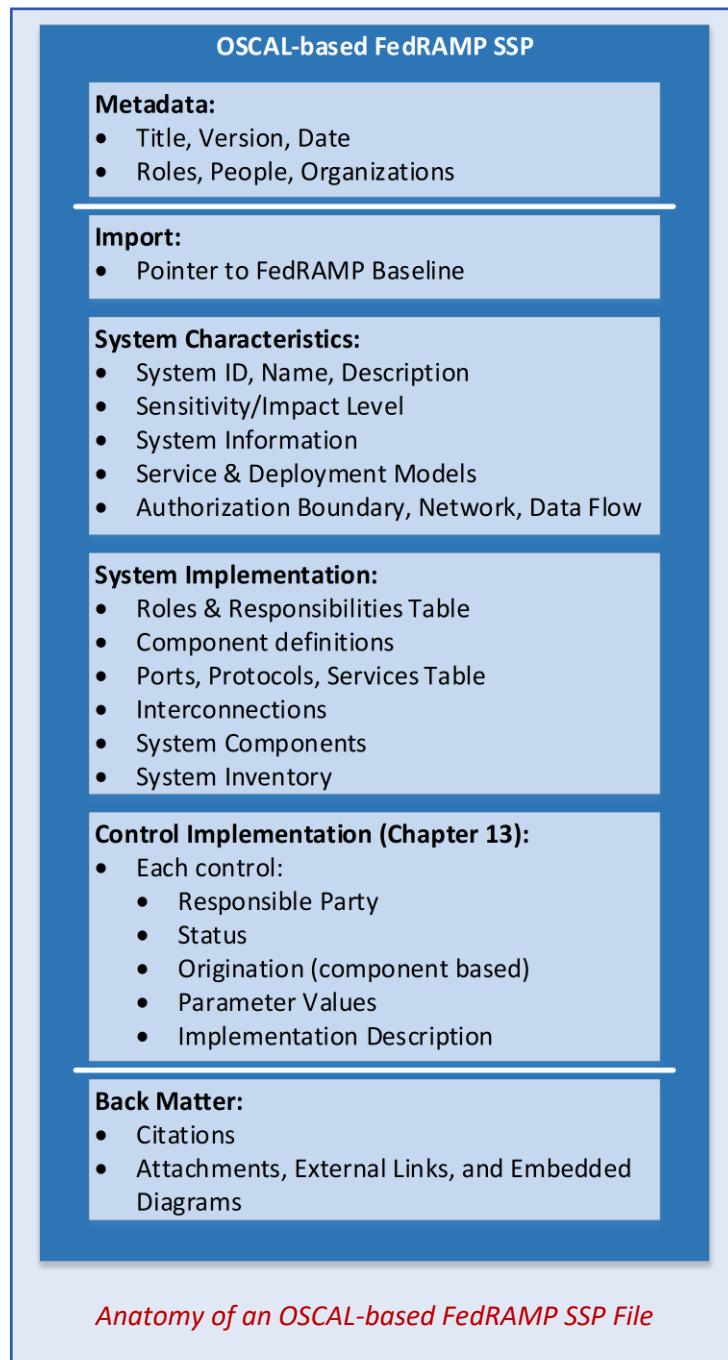
FedRAMP requires all layers be satisfied.

LAYER	DESCRIPTION
Well-Formed	The XML or JSON file follows the rules defined for that format. Any tool that processes the format will recognize it as “well-formed”, which means the tool can proceed with processing the XML or JSON. XML: https://www.w3.org/TR/REC-xml/ JSON: https://json.org/
OSCAL Syntax	The XML or JSON file only uses tagging that is defined by NIST for OSCAL. NIST publishes schema validation tools to verify syntax compliance: XML Schema Definition Language (XSD) 1.1 : OSCAL SSP XML Validation File JSON Schema, draft 07 : OSCAL SSP JSON Validation File
OSCAL Content	Currently NIST only enforces declarations, using the validation files above. This means defining a limited set of acceptable values for certain fields. For example, NIST declared the following as the only acceptable values for the impact levels for information types: “fips-199-low”, “fips-199-moderate”, and “fips-199-high”. Any other value will raise an error when validating the file using the NIST schema tools above. In the future, NIST intends to publish content enforcement mechanisms, such as Schematron . This will enforce more complex rules such as, “If field A is marked ‘true’, field B must have a value.”
FedRAMP Syntax Extensions	NIST built a language they believe represents the commonality of most cybersecurity frameworks and provided the ability to extend the language for framework-specific needs. FedRAMP makes use of these extensions. NIST provides <code>prop</code> and <code>annotation</code> fields throughout its most assemblies, always with a <code>name</code> , <code>class</code> , and <code>ns</code> (namespace) flag: <code><prop name="" class="" ns="">Data</prop></code> In the core OSCAL syntax, the <code>ns</code> flag is never used. Where FedRAMP uses these to extend OSCAL, the value for <code>ns</code> is always: https://fedramp.gov/ns/oscal (case sensitive). When <code>ns='https://fedramp.gov/ns/oscal'</code> the <code>name</code> flag is as defined by FedRAMP. If the <code>class</code> flag is present, that is also defined by FedRAMP.
FedRAMP Content	Today, FedRAMP content is enforced programmatically. FedRAMP will evaluate the use of Schematron (above) for future FedRAMP validation efforts.

2.3. OSCAL's Minimum File Requirements

Every OSCAL-based FedRAMP SSP file must have a minimum set of required fields/assemblies, and must follow the OSCAL SSP core syntax found here:

<https://pages.nist.gov/OSCAL/documentation/schema/ssp/>



In addition to the core OSCAL syntax, the following FedRAMP-specific implementation applies:

- A FedRAMP SSP must include all the sections shown in the diagram to the left.
- At a minimum, the FedRAMP SSP must have at least one defined component, which represents the system as a whole. This is addressed in more detail in the system inventory.
- A leveraged authorization is defined as a component, if the system is leveraging another FedRAMP-authorized system.

The table below shows an empty OSCAL SSP, based purely on the NIST syntax; however, FedRAMP requires much more in a minimum file. The latest OSCAL-based FedRAMP SSP template file can be found here in JSON and XML formats:

<https://github.com/GSA/fedramp-automation/tree/master/templates>

An Empty OSCAL SSP Representation
<pre> <?xml version="1.0" encoding="UTF-8"?> <system-security-plan xmlns="http://csrc.nist.gov/ns/oscal/1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="[generated-uuid-here]"> <metadata> <title>System Security Plan (SSP)</title> <last-modified>2019-11-27T00:00:00.00-05:00</last-modified> <version>0.0</version> <oscal-version>1.0-Milestone2</oscal-version> </metadata> <import-profile href="baseline-profile.xml" /> <system-characteristics> <system-id>Unique System Identifier</system-id> <system-name>System's Name</system-name> <description><p>Description of system's Name</p></description> <security-sensitivity-level>moderate</security-sensitivity-level> <system-information> <information-type id="info-type-01" name="Name"> <description><p>Description</p></description> <confidentiality-impact> <base>fips-199-moderate</base> </confidentiality-impact> <integrity-impact> <base>fips-199-moderate</base> </integrity-impact> <availability-impact> <base>fips-199-moderate</base> </availability-impact> </information-type> </system-information> <security-impact-level /> <status state="operational" /> <authorization-boundary> <description><p>Description</p></description> </authorization-boundary> </system-characteristics> <back-matter /> </system-security-plan> </pre>

NOTES:

- The first line ensures UTF-8 is used for character encoding. Other encoding options will create unpredictable results.
- A new UUID must be generated every time the file is changed.
- The last-modified date must be updated every time the file is changed.

Below are a few important queries, which enable a tool to obtain critical information about an OSCAL file.

XPath Queries
OSCAL syntax version used in this file: /*/metadata/oscal-version
Last Modified Date/Time: /*/metadata/last-modified
Unique Document ID: /system-security-plan/@id
Document Title: /*/metadata/title

NOTES:

- For full OSCAL compliance, **any time the document changes**:
 - the file's `id` flag (`/system-security-plan/@id`) should be updated with a new unique identifier; and
 - the `last-modified` field should be updated with the current date and time.
- Tools that work with updates to an OSCAL file should rely on the UUID value provided by the `id` flag, and `last modified` field as an easy method of knowing the file has changed.
- NIST intends to add a cryptographic hash feature in the future; however, this is not available today.
 - While tool developers are encouraged to perform as much integrity checking as possible, it is important to note the content of a JSON or XML file may not have changed, yet a different cryptographic hash could be produced as a result of formatting, which might have different indentation, or change the sequence of flags.
- Tools reading an OSCAL file should verify the `oscal-version` field to determine which published syntax is used.
 - NIST intends to enable backward compatibility as much as possible; however, this is not guaranteed. Especially before a full final 1.0 version of OSCAL.
 - NIST intends to keep all formally published schema validation files available, which enables an organization to validate files based on older versions of OSCAL.

2.4. Assigning Identifiers

There are three ways identifiers are typically used in OSCAL:

- **ID flag**: uniquely identifies a field or assembly.
- **ID Reference**: a flag or field that points to another field or assembly using its ID unique flag value.
- **Uniform Resource Identifier (URI) Fragment**: A value in a flag or field with a [URI data type](#). A [URI fragment](#) starts with a hashtag (#) followed by a unique ID value.

ID flags appear as an “`id`” flag to a data field or assembly. Examples include:

- `<interconnection id="ic-001">`: Uniquely identifies the interconnection
- `<party id="csp">`: Uniquely identifies the party

An ID reference typically appears with a name and hyphen in front of the “`id`” (name-id). It is typically a flag, but sometimes a field. The name of an ID reference flag/field typically reflects the name of the field to which it points.

Examples include:

- `<responsible-party role-id="prepared-by">`: points to a `role` identified by “`prepared-by`”.
- `<implemented-requirement id="imp-req-01" control-id="ac-2">`: points to the `control` identified by “`ac-2`”.

Throughout the OSCAL syntax, if an ID flag is available, it is typically required.

NIST provides some standard identifiers. Where appropriate, FedRAMP has adopted those and defined additional identifiers as needed. To ensure consistent processing, FedRAMP encourage content creators to use the NIST and FedRAMP-defined identifiers to the greatest degree practical. Deviation is likely to result in processing errors.

2.4.1. Uniqueness of Identifiers

OSCAL syntax validation tools currently require an identifier to be unique among like-named fields. For example, the same ID value must not be present for two different `role` fields; however, the ID value for a `party` field may be the same as the ID value for a `role` field.

As a best practice, the FedRAMP PMO recommends ensuring IDs are unique within the file as a whole, and not just within the scope of like-named elements.

This is especially important if using Uniform Resource Identifier (URI) fragments in URI fields such as `href="#id-value"`. NIST does not yet have clear rules for handling URI fragments when the referenced id-value appears more than once in the file. Keeping IDs unique within the file avoids URI fragment ambiguity. If you chose to reuse ID values across non-like-named fields, consider only using URI fragments in `href` fields that point to resource assemblies.

When resolving a URI fragment for an ID that exists more than once in the file, the FedRAMP PMO encourages tool developers to have their tools evaluate whether an ID points to a resource first.

2.5. Handling of OSCAL Data Types

OSCAL fields and flags have data types assigned to them. NIST provides important information about these data types here:

<https://pages.nist.gov/OSCAL/documentation/schema/datatypes/>

The following sections describe special handling considerations for data types that directly impact FedRAMP SSP content in OSCAL.

2.5.1. Date and Time in OSCAL Files

Except where noted, all dates and times in the OSCAL-based SSP must be in an OSCAL date-time-with-timezone format as documented here:

<https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#datetime-with-timezone>

This means all dates and times must be represented in the OSCAL file using following format, unless otherwise noted:

"Y-m-d\TH:i:s.uP" (See [HERE](#) for formatting codes.)

For example, a publication date of 5:30 pm EST, January 10, 2020 must appear as
2020-01-10T17:30:00.00-05:00

This includes:

- Numeric Year: Four-digits
- A dash
- Numeric Month: Two-digit, zero-padded
- A dash
- Numeric Day: Two digit, zero padded
- The capital letter "T" (Do not use lower case)
- Hour: Two digit, zero-padded, 24-hour clock (Use 18 for 6:00 pm)
- A colon
- Minute: Two digit, zero-padded
- A colon
- Seconds: Two digit, zero-padded
- A decimal point
- Fractions of a second: two or three digits, zero padded

Followed by either:

- A capital letter Z to indicate the time is expressed in Coordinated Universal Time (UTC)

OR:

- A plus or minus representing the offset from UTC
- Hour Offset: Difference from UTC, two-digit, padded
- A colon
- Minutes Offset: Difference from UTC, two-digit, padded

This is only for *storing* dates in the OSCAL file. NIST syntax verification tools will generate an error if this format is not found.

Tool developers are encouraged to *present* dates as they have historically appeared in the FedRAMP SSP template. In other words, tools should convert "2020-03-04T00:00:00.00-05:00" to "March 4, 2020" when presenting the publication date to the user.

Please use the appropriate UTC offset in your region. If you are storing a date and padding the time with zeros, you may also pad the UTC offset with zeros.

2.5.2. Working With href Flags

Several OSCAL fields contain `href` flags. All OSCAL-based `href` flags are uniform resource identifiers (URIs) formatted according to [section 4.1 of RFC3986](#). When assembling or processing an OSCAL-based FedRAMP SSP please consider the following:

Absolute Paths: When using an absolute path within a FedRAMP SSP, the path must be publicly accessible from any location on the Internet, to ensure agency and FedRAMP reviewers can reach the information.

Tool developers are encouraged to validate paths before storing them in OSCAL files and raise issues to users if paths are not reachable.

Relative Paths: All relative paths are assumed to be based on the location of the OSCAL file, unless tools are explicit as to other handling. Sensitive external documents should travel with the SSP and be linked using a relative path.

Internal Locations: These URI fragments appear as just a hashtag (#) followed by a name, such as "#att-diagram-1". The notation points to a location internal to the document itself and is most commonly used in an OSCAL-based FedRAMP SSP as a pointer to `resource` assemblies.

If only a fragment is present, the OSCAL tools must strip the hashtag (#) and treat the remaining string as an ID internal to the OSCAL file itself. For example, the following OSCAL content contains an `href` flag with a URI fragment:

URI Fragment Example

```
<system-characteristics>
    <authorization-boundary>
        <diagram id="dia-authorization-boundary-1">
            <link href="#att-diagram-boundary-1"/>
            <caption>Authorization Boundary Diagram</caption>
        </diagram>
    </authorization-boundary>
</system-characteristics>
```

When a tool processes the above example, it should look inside the document for a field or assembly with an ID of "att-diagram-boundary-1". This can be accomplished with the following XPath query:
`//*[@@id="att-diagram-boundary-1"]`

If this is found to point to a resource assembly, see the *Attachments and Embedded Content in OSCAL Files* section for additional handling.

The name of the field or assembly referenced by the above URI fragment can be determined using the following XPath 2.0 query:

```
// *[@id="att-diagram-boundary-1"] /name ()
```

To express this in XPath 1.0, you must use the following:

```
name (// *[@id="att-diagram-boundary-1"] )
```

The above query will return "resource", if the ID points to a `resource` assembly.

2.5.3. Markup-line and Markup-multiline Fields in OSCAL

As with most machine-readable formats, most of OSCAL's fields are intended to capture short, discrete pieces of information; however, sometimes users require content to be formatted using features such bold, underline, and italics.

OSCAL provides two types of fields for this purpose:

- **markup-line**: Allows some formatting within a single line of text.
- **Markup-multiline**: Allows all the markup-line formatting, plus allows multiple lines, ordered/unordered lists, and tables.

A subset of HTML is used to format XML-based OSCAL files, while Markdown is used to format JSON-based OSCAL files.

NIST has implemented only a subset of formatting tags from these standards. This is to ensure formatted content converts between XML and JSON consistently.

Both *markup-line* and *markup-multiline* support:

- emphasis and important text
- inline code and quoted text
- sub/super-script
- images and links

Markup-multiline also supports:

- Paragraphs
- Headings (Levels 1-6)
- Preformatted text
- Ordered and Unordered Lists
- Tables

For markup-line and markup-multiline, a subset of HTML is used to format XML-based OSCAL files, while Markdown is used to format JSON-based OSCAL files.

For a complete list of markup-line and markup-multiline features, please visit:

<https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-data-types>

2.5.4. Working with Markup-multiline Content

OSCAL's markup-multiline No special handling is required to work with markup-multiline content in JSON; however, XML-based markup-multiline fields require all content to be enclosed in `<p>`, `<h1>` – `<h6>`, ``, ``, `<pre>`, or `<table>` tags. You may have several of these within the field.

The following examples offer correct and incorrect representations of Markup-multiline content.

The example below is a common miss-use of markup-multiline. The description contains text, but the text is not enclosed in one of the required tags. This will produce an error when checked with the OSCAL schema.

Incorrect Markup-multiline Representation

```
<system-characteristics
    <!-- cut -->
    <description>The xyz system performs ...</description>
</system-characteristics>
```

The simplest way to correct the error is to enclose the text in `<p></p>` tags, within the `description` field.

Correct Markup-multiline Representation

```
<system-characteristics
    <!-- cut -->
    <description><p>The xyz system performs ...</p></description>
</system-characteristics>
```

The example below demonstrates a correct use of markup-multiline in XML. Please note, the inclusion of a `<p />` tag on a line by itself inserts an empty paragraph. Within XML and HTML, this is treated as a shortcut, and is interpreted as "`<p></p>`"

Correct Markup-multiline Representation

```
<system-characteristics
    <!-- cut -->
    <description>
        <p>The <b>xyz system</b> performs ...</p>
        <p>The xyz system further supports ... as follows:</p>
        <table>
            <tr>
                <td>Cell A1</td>
                <td>Cell B1</td>
            </tr>
            <tr>
                <td>Cell A2</td>
                <td>Cell B2</td>
            </tr>
        </table>
        <h1>Big Header</h1>
        <p>More detail</p>
        <p></p>
    </description>
</system-characteristics>
```

Please also note, all content is enclosed in one of the supported high-level tags (`<p>`, `<h1>` – `<h6>`, ``, ``, `<pre>`, or `<table>`).

For more information, please visit:

<https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-data-types>

2.5.5. Special Characters in OSCAL

While OSCAL itself does not directly impose special character handling requirements, XML and JSON do. Characters, such as ampersand (&), greater than (>), less than (<), and quotes ("") require special treatment in OSCAL files, depending on the format. For a complete list of special characters and the appropriate treatment for each format, please visit:

<https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#specialized-character-mapping>

2.6. Citations, Attachments and Embedded Content in OSCAL Files

All citations, attachments, and embedded content are handled in the back-matter section of the OSCAL file as a `citation` or `resource` assembly. This includes logos, diagrams, policies, procedures, plans, and interconnection security agreements (ICAs). Each `citation` or `resource` may be referenced from anywhere in the OSCAL file, using its citation ID or resource ID. FedRAMP prefers Base64-encoding for diagrams, such as those related to the authorization boundary, network architecture, and data flows.

```
<back-matter>
    <!-- citation -->
    <resource id="csp-logo">
        <desc>CSP Logo</desc>
        <rlink href="../logo.png" media-type="image/png" />
        <rlink href="../logo.jpg" media-type="image/jpeg" />
        <base64>--- base64 content cut ---</base64>
    </resource>
</back-matter>
```

Resources may be expressed as:

- a link to external file (`rlink`);
- base64-encoded data within the OSCAL file;
- both; or
- neither.

OSCAL allows multiple `rlink` fields for the same resource, which are intended to provide options such as links to the same content in different formats, or low- and high-resolution versions of the same graphic.

There is no OSCAL rule which governs how a tool should handle a situation where both the `rlink` and `base64` fields and/or where multiple `rlink` fields are present for a single resource.

FedRAMP tools will always give preference to base64-encoded content. If the `base64` field is present with valid content, FedRAMP tools will ignore all `rlink` fields.

If the `base64` field is missing or invalid, FedRAMP tools will try the first `rlink` field. If that works, all remaining `rlinks` will be ignored. If the first one does not work, FedRAMP tools will try the second link, then the third. It will keep going until either a valid rlink is found, or no rlink fields remain.

CSPs should take care when using `rlink` fields to ensure all paths are relative to the OSCAL file's location itself, and the referenced items delivered to FedRAMP with the OSCAL file.

The `resource` assembly could be used with neither `rlink` nor `base64` embedded content. If citing a document that may be attached or embedded later, this approach may be used as a placeholder. If citing a document that will never be attached or embedded, use the `citation` assembly instead.

Using either the `citation` or `resource` assembly with the FedRAMP's additional properties (title, publication, and version), enables a CSP to reference a document by title, version, and date in one place, then reference it where needed throughout the OSCAL file. This way, the title, version and date can be updated in one place and will appear updated everywhere it is referenced.

3. FEDRAMP EXTENSIONS, DEFINED IDENTIFIERS, AND ACCEPTED VALUES

NIST designed the core OSCAL syntax to meet model cybersecurity information that is common to any organization and compliance framework. They recognized that each framework and organization may have unique needs. Instead of trying to provide a language that meets each of those unique needs, NIST gave organizations the ability to tailor OSCAL to address specific needs.

A summary of the FedRAMP extensions, defined identifiers, and accepted values appears in the FedRAMP OSCAL Registry.

FedRAMP has tailored OSCAL by specifying:

- **Extensions:** allow FedRAMP's OSCAL-based SSP to capture information that is not available in the core OSCAL SSP syntax.
- **Defined Identifiers:** FedRAMP defines several unique ID values that must be used in the ID flag of certain OSCAL fields and assemblies. This allows FedRAMP processing tools to find required information without human intervention.
- **Accepted Values:** For many fields, FedRAMP specifies a case-sensitive set of values. Only these values are recognized by FedRAMP processing tools.

3.1.1. FedRAMP Extensions

There are several pieces of information required in a FedRAMP SSP that cannot be modeled using OSCAL's core syntax. NIST wanted to limit the core OSCAL syntax to those elements that are universal across most cybersecurity frameworks. They designed OSCAL to be extended where unique needs existed.

All FedRAMP extensions include a namespace (ns) flag set to " https://fedramp.gov/ns/oscal".

NIST allows organizations to extend OSCAL anywhere `prop` fields, `part` assemblies, or `annotation` assemblies exist in the core syntax. (Please note, there are currently no `part` assemblies in the SSP model.) There are two fundamental requirements for extending OSCAL:

- The organization must establish a unique namespace (ns) identifier, such as (`ns="http://domain.org/ns/oscal"`), and use it to consistently tag all `prop`, `part`, and `annotation` extensions from that organization.
- The organization is responsible for defining, managing, and communicating all names (`name="scan-type"`) defined and tagged with the above name space identifier.

NIST's core OSCAL `prop` fields and `annotation` assemblies have no `ns` flag. If an `ns` flag is present, it is an organization-defined extension. This allows each industry standards body or organization to create their own extensions in their own name space without concern for overlapping names.

The above approach ensures two different organizations can create their own extensions without concern for reusing the same name values. At some point in the future, NIST may provide a registry for organizational extensions. For now, FedRAMP is publishing its own [registry](#) to document its extensions.

All FedRAMP extensions include a namespace (ns) flag set to " <https://fedramp.gov/ns/oscal>".

For example, if the core OSCAL syntax has a status field, but both FedRAMP and the payment card industry (PCI) require their own framework-specific `user` field, each may define an extension with the `name="name"`, and assign their own `ns` flag. This results in three possible status fields as follows:

NIST OSCAL User Representation

```
<prop name="user">User as intended by OSCAL core syntax</prop>
```

XPath Query

```
//prop[@name="user"] [not(@ns)]
```

When searching an OSCAL file for a `prop` or `annotation` extensions that is part of the core OSCAL syntax, developers must filter out any with an `ns` flag using the syntax above.

FedRAMP User Representation

```
<prop name="user" ns="https://fedramp.gov/ns/oscal">FedRAMP User</prop>
```

XPath Query

```
//prop[@name="user"] [@ns="https://fedramp.gov/ns/oscal"]
```

(Possible) PCI User Representation

```
<prop name="user" ns="https://pcisecuritystandards.org/ns/oscal">PCI User</prop>
```

XPath Query

```
//prop[@name="user"] [@ns="https://pcisecuritystandards.org/ns/oscal"]
```

* This is an example, and not intended to represent an actual PCI extension.

Tool developers must always refer to extensions using **both** the `name` and `ns` flags as a pair.

All FedRAMP extensions will appear as either:

```
<prop name=" " ns="https://fedramp.gov/ns/oscal">Value</prop>
```

or:

```
<annotation name=" " ns="https://fedramp.gov/ns/oscal" value="Value">
  <remarks><p>A possible remark about the value</p></remarks>
</annotation>
```

NOTE: The catalog and profile OSCAL models also allow the `part` assembly to be used for extensions. This is not currently the case for the SSP OSCAL model.

FedRAMP extensions are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

3.1.2. FedRAMP Defined Identifiers

To facilitate consistent processing, FedRAMP requires specific identifiers be used on several fields/assemblies within the OSCAL file.

For example, every SSP must identify a system owner and an Information System Security Officer (ISSO). FedRAMP defines specific identifiers for these roles, and enables FedRAMP tools to easily identify the individuals associated with these roles.

FedRAMP defined identifiers are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

3.1.3. OSCAL and FedRAMP Accepted Values

To facilitate consistent processing, the value for some fields is limited to a list of *case-sensitive* acceptable values. For some fields, OSCAL defines acceptable values, which are enforced by OSCAL-based syntax validation mechanisms.

There are additional fields, where OSCAL syntax validation mechanisms will accept any value, but FedRAMP provides a limited list of *case-sensitive* acceptable values. Where defined, only these values are recognized by FedRAMP processing tools.

For example, every control requires an implementation status. FedRAMP only accepts one of five possible responses for this status, which must be provided using one of the specified choices.

FedRAMP accepted values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

4. SSP TEMPLATE TO OSCAL MAPPING

Each page of the SSP where content is provided by a CSP is represented in this section, along with OSCAL code snippets for representing the information in OSCAL syntax. There is also XPath syntax for querying the code in an OSCAL-based FedRAMP SSP represented in XML format.

The following pages are intended to be printed landscape on tabloid (11" x 17") paper.

FEDRAMP SYSTEM SECURITY PLAN (SSP) BASELINE TEMPLATE

Cloud Service Provider Name
Information System Name
Version #
Version Date



The **FedRAMP Logo** is base 64 encoded in the back-matter section of the OSCAL-based FedRAMP SSP Template, and can be referenced with the following XPath:
`//back-matter/resource[@id='logo-fedramp']/base64`

CONTROLLED UNCLASSIFIED INFORMATION

4.1. SSP Title Page

Representation

```
<metadata>
    <title>FedRAMP System Security Plan (SSP)</title>
    <published>2019-10-21T00:00:00.00-04:00</published>
    <last-modified>2019-11-27T00:00:00.00-04:00</last-modified>
    <version>0.0</version>
    <oscal-version>1.0-Milestone2</oscal-version>
    <prop name="marking" ns="https://fedramp.gov/ns/oscal">Controlled Unclassified
Information</prop>
    <!-- role -->
    <party id="csp">
        <org>
            <org-name>Cloud Service Provider (CSP) Name</org-name>
            <short-name>CSP Acronym/Short Name</short-name>
        </org>
    </party>
    <!-- responsible-role -->
</metadata>
```

FedRAMP Extension (Document Marking)

- prop(ns="https://fedramp.gov/ns/oscal"):
- name="marking"

```
<!-- This must point to the appropriate FedRAMP Baseline -->
<import-profile href="https://path/to/FedRAMP_MODERATE-baseline_profile.xml"/>

<system-characteristics
    <system-id identifier-type="https://fedramp.gov">F00000000</system-id>
    <system-name>System's Full Name</system-name>
    <system-name-short>System's Short Name or Acronym</system-name-short>
    <!-- description -->
</system-characteristics>
```

XPath Queries

CSP Name:
`/*/metadata/party[@id='csp']/org/org-name`

Information System Name:
`/*/system-characteristics/system-name`

SSP Document Published Version #:
`/*/metadata/version`

SSP Document Published Date:
`/*/metadata/published`

CSP's Logo:
`/*/back-matter/resource[@id='logo-csp']/base64`

Document Sensitivity Label:
`/*/metadata/prop[@name="marking"][@ns="https://fedramp.gov/ns/oscal"]`

NOTES:

- The import-profile field is required. There must always be a profile imported. All of the control definition statements, and parameter descriptions are imported via that profile.
- The correct URLs for each FedRAMP baseline appear in Appendix A. There are separate XML and JSON URLs for each baseline.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

SYSTEM SECURITY PLAN

Prepared by

Identification of Organization that Prepared this Document	
	Organization Name <Enter Company/Organization>.
	Street Address <Enter Street Address>
	Suite/Room/Building <Enter Suite/Room/Building>
	City, State Zip <Enter Zip Code>

Prepared for

Identification of Cloud Service Provider	
	Organization Name <Enter Company/Organization>.
	Street Address <Enter Street Address>
	Suite/Room/Building <Enter Suite/Room/Building>
	City, State Zip <Enter Zip Code>

TEMPLATE REVISION HISTORY

Date	Description
6/1/2018	Initial version of the template.
6/1/2019	Template Revision History is obsolete with OSCAL.
6/1/2020	Instead refer to the OSCAL syntax version.
8/1/2020	to SA -9, updated requirements in RA-5

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

Controlled Unclassified Information

4.2. SSP Prepared By/For

Representation

```
<metadata>
    <!-- prop -->
    <role id="prepared-by">
        <title>Prepared By</title>
        <desc>The organization that prepared this SSP.</desc>
    </role>
    <role id="prepared-for">
        <title>Prepared For</title>
        <desc>The organization for which this SSP was prepared.</desc>
    </role>
    <!-- cut -->
    <party id="csp">
        <org>
            <org-name>Cloud Service Provider (CSP) Name</org-name>
            <short-name>CSP Acronym/Short Name</short-name>
            <address>
                <!-- address lines cut here for space -->
            </address>
        </org>
    </party>
    <responsible-party role-id="prepared-by">
        <party-id>csp</party-id>
    </responsible-party>
    <responsible-party role-id="prepared-for">
        <party-id>csp</party-id>
    </responsible-party>
</metadata>
<!-- cut -->
<back-matter>
    <!-- citations -->
    <resource id="logo-csp">
        <desc>CSP Logo</desc>
        <rlink href="../logo.png" media-type="image/png" />
        <base64 filename='logo.png'>--- base64 content cut ---</base64>
    </resource>
</back-matter>
```

NIST-Defined Identifiers

- prepared-by
 - prepared-for

FedRAMP-Defined Identifier

- csp

Required Resource ID:

 - csp-logo

XPath Queries

CSP's Logo:

```
    /*/back-matter/resource[@id='logo-csp']/base64  
    /*/back-matter/resource[@id='logo-csp']/rlink/@href
```

Prepared By: Details:

```
/*metadata/party[@id=[/*metadata/responsible-party[@role-id='prepared-by']/party-id]/org/org_name
```

Prepared For Details:

```
/*/metadata/party[@id=/*/metadata/responsible-party[@role-id='prepared-for']/party-  
id]/name
```

NOTE: Replace "org-name" with "address/addr-line", "address/city", "address/state", or "address/zip" as needed. There may be more than one addr-line.

NOTES.

- If this was prepared by a 3PAO, their logo should also be a resource in the back-matter with a resource ID of 'logo-3pao', and that ID should be used here in place of 'logo-csp' for Prepared By.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact info@FedRAMP.gov

For more information about the FedRAMP project, see www.FedRAMP.gov

Instruction: The System Security Plan is the main document in which the Cloud Service Provider (CSP) describes all the security controls in use on the information system and their implementation.

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).

In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Note that "-1" Controls (AC-1, AU-1, SC-1, etc.)* cannot be inherited and must be described in some way by the service provider.

*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For System as a Service (SaaS) and Platform as a Service (PaaS) systems that are inheriting controls from an Infrastructure as a Service (IaaS) (or anything lower in the stack), the "inherited" check box must be checked and the implementation description must simply say "inherited." FedRAMP reviewers will determine whether the control-set is appropriate or not.

4.3. Document Revision History

Document revision history is not yet available in OSCAL. NIST intends to include it in Milestone Release 3 (MR-3).

This space is a placeholder and will be updated, once that feature is available.

4.4. How to Contact Us

The FedRAMP email and web site addresses are part of the organizational content for the FedRAMP PMO.

Representation

```
...<metadata>
    <!-- role -->
    <party id="fedramp-pmo">
        <org>
            <org-name>Federal Risk and Authorization Management Program: PMO</org-name>
            <short-name>FedRAMP PMO</short-name>
            <address>
                <addr-line>1800 F St. NW</addr-line>
                <city>Washington</city>
                <state>DC</state>
                <postal-code></postal-code>
                <country>us</country>
            </address>
            <email>info@fedramp.gov</email>
            <url>https://fedramp.gov</url>
        </org>
    </party>
    <party id="fedramp-jab">
        <org>
            <org-name>FedRAMP Joint Authorization Board</org-name>
            <short-name>FedRAMP JAB</short-name>
        </org>
    </party>
    <!-- responsible-party -->
...<metadata>
```

XPath Queries

FedRAMP email address:
`/*/metadata/party[@id='fedramp-pmo']/org/email`

FedRAMP web site:
`/*/metadata/party[@id='fedramp-pmo']/org/url`

FedRAMP-Defined Identifiers

Required Party IDs:

- fedramp-pmo
- fedramp-jab

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE
CSP Name | Information System Name Version #., Date

System Security Plan Approvals

Cloud Service Provider Signatures

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Cloud Service Provider	CSP Name		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Cloud Service Provider	CSP Name		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Cloud Service Provider	CSP Name		

FedRAMP 0100011001000101010001000100100100000101000110101010000010011110101
Controlled Unclassified Information

4.5. System Security Plan Approvals

Representation

```

<metadata>
  <!-- prop, link -->
  <role id="content-approver">
    <title>System Security Plan Approval</title>
    <desc>The individual or individuals within the CSP authorized to take
          responsibility for the accuracy of this SSP.</desc>
  </role>
  <!-- cut -->
  <party id="person-1">
    <person>
      <person-name>Name 1</person-name>
      <org-id>csp</org-id>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Job Title</prop>
    </person>
  </party>
  <party id="person-2">
    <person>
      <person-name>Name 2</person-name>
      <org-id>csp</org-id>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Job Title</prop>
    </person>
  </party>
  <!-- cut -->
  <responsible-party role-id="content-approver">
    <party-id>person-1</party-id>
    <party-id>person-2</party-id>
  </responsible-party>
  <!-- remarks (or nothing else under metadata) -->
</metadata>

```

NIST-Defined Identifier

Required Party ID:

- content-approver

FedRAMP Extension (Person's Title)

prop(ns="https://fedramp.gov/ns/oscal"):

- name="title"

XPath Queries

Approver's Name:

```
(/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id='content-
approver']] /party-id]]/person/person-name) [1]
```

Approver's Title:

```
(/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id='content-
approver']] /party-
id]]/person/prop[@name='title'] [@ns='https://fedramp.gov/ns/oscal']) [1]
```

NOTE: For each additional approver, replace the "[1]" with "[2]", "[3]", and so on.

CSP Name:

```
/*/metadata/party[@id='csp'] /org/org-name
```

NOTES:

- A person's title is not a valid OSCAL field. This uses a FedRAMP extension to capture a person's title.
- The code above shows two approvers. At least one is required. There is no limit to the number of approvers; however, FedRAMP encourages no more than three.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

I. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the Information System Name (Enter Information System Abbreviation) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the Enter Information System Abbreviation information system.

The security safeguards implemented for the Enter Information System Abbreviation system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table I-1. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
<Enter FedRAMP Application Number>	Information System Name	Enter Information System Abbreviation

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

Controlled Unclassified Information

4.6. Information System Name, Title, and FedRAMP Identifier

The FedRAMP-assigned application number is the unique ID for a FedRAMP system. OSCAL supports several system identifiers, which may be assigned by different organizations.

For this reason, OSCAL requires the `identifier-type` flag be present and have a value that uniquely identifies the issuing organization. FedRAMP requires its value to be "<http://fedramp.gov>" for all FedRAMP-issued application numbers.

Representation

```
<system-characteristics>
  <system-id identifier-type="http://fedramp.gov">F00000000</system-id>
  <system-name>System's Full Name</system-name>
  <system-name-short>System's Short Name or Acronym</system-name-short>
  <!-- description -->
</system-characteristics>
```

NIST-Defined Identifier

Required Identifier Type:

- `identifier-type="http://fedramp.gov"`

XPath Queries

FedRAMP System Identifier:

`/*/system-characteristics/system-id[@identifier-type="https://fedramp.gov"]`

Information System Name:

`/*/system-characteristics/system-name`

Information System Abbreviation:

`/*/system-characteristics/system-name-short`

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

2. INFORMATION SYSTEM CATEGORIZATION

The overall information system sensitivity categorization is recorded in Table 2-1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Attachment 10. FIPS 199.**

Table 2-1. Security Categorization

System Sensitivity Level:	Choose level.
---------------------------	---------------

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101
Controlled Unclassified Information

4.7. Information System Categorization and FedRAMP Baselines

Table 2-1 and Table 2-4 Representation

```
<system-characteristics>
  <!-- description -->
  <prop name="authorization-type" ns="https://fedramp.gov/ns/oscal">fedramp-
agency</prop>
  <!-- annotation, link, date-authorized -->
  <security-sensitivity-level>moderate</security-sensitivity-level>
  <!-- system-information -->
</system-characteristics>
```

FedRAMP Extensions & Accepted Values

```
prop (ns="https://fedramp.gov/ns/oscal"):
  • name="authorization-type"
    o Valid: fedramp-jab, fedramp-agency,
      fedramp-li-saas
```

OSCAL Accepted Values

Valid values for security-sensitivity-level:

- low
- moderate
- high

XPath Queries

System Sensitivity Level:
`/*/system-characteristics/security-sensitivity-level`

URL to OSCAL-based FedRAMP Baseline File:
`/*/import-profile/@href`

FedRAMP Authorization Type:
`/*/system-characteristics/prop[@name="authorization-
type"][@ns="https://fedramp.gov/ns/oscal"]`

NOTES:

- The identified System Sensitivity Level governs which FedRAMP baseline applies. See Appendix A for more information about importing the appropriate FedRAMP baseline.

The adjustment-justification fields are <i>Markup multiline</i> , which enables the text to be formatted. This requires special handling. See <i>Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</i> , or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline	Date			
FedRAMP Accepted Values FedRAMP only accepts NIST SP 800-60 IDs. The system flag of the information-type-id field must be: <ul style="list-style-type: none">• https://doi.org/10.6028/NIST.SP.800-60v2r1	as needed to add and Systems to			
Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
System Development	C.3.5.1	Low	Moderate	Low

Table 2-2. Sensitivity Categorization of Information Types

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.

Table 2-2 is a sub-set of Table 15-9 as follows:

Table Column	Table 2-2	Table 15-9	XPath Queries
Information Type	Yes	Yes	//system-characteristics/system-information/information-type[1]/@name
NIST 800-60 Identifier	Yes	Yes	//system-characteristics/system-information/information-type[1]/information-type-id[@system="nist"]
NIST Recommended Confidentiality Impact Level	No	Yes	//system-characteristics/system-information/information-type[1]/confidentiality-impact/base
NIST Recommended Integrity Impact Level	No	Yes	//system-characteristics/system-information/information-type[1]/integrity-impact/base
NIST Recommended Availability Impact Level	No	Yes	//system-characteristics/system-information/information-type[1]/availability-impact/base
CSP Selected Confidentiality Impact Level	Yes	Yes	//system-characteristics/system-information/information-type[1]/confidentiality-impact/selected
CSP Selected Integrity Impact Level	Yes	Yes	//system-characteristics/system-information/information-type[1]/integrity-impact/selected
CSP Selected Availability Impact Level	Yes	Yes	//system-characteristics/system-information/information-type[1]/availability-impact/selected
Impact Adjustment Justification	No	Yes	//system-characteristics/system-information/information-type[1]/confidentiality-impact/adjustment-justification //system-characteristics/system-information/information-type[1]/integrity-impact/adjustment-justification //system-characteristics/system-information/information-type[1]/availability-impact/adjustment-justification

In each XPath query in the table above, replace the "[1]" with "[2]", "[3]", as needed, up to the number of information-type fields that exist in the file.

Use the following XPath statement to count the number of information-type fields: `count("//system-characteristics/system-information/information-type")`

The FedRAMP SSP Template has only one place to provide the justification of changing any of the three recommended NIST 800-60 levels. OSCAL ties this justification to its individual type (confidentiality, availability, or integrity). If recreating Table 15-9 from OSCAL data, display all three justifications in this single field, and label each.

4.8. Information Types

Table 2-2 and Table 15-9 Representation

```

<system-information>
  <!-- security-sensitivity-level -->
  <information-type name="Information Type Name" id="info-01">
    <information-type-id system="https://doi.org/10.6028/NIST.SP.800-60v2r1">
      C.2.4.1</information-type-id>

    <confidentiality-impact>
      <base>fips-199-moderate</base>
      <selected>fips-199-moderate</selected>
      <adjustment-justification><p>Description</p></adjustment-justification>
    </confidence-impact>
    <integrity-impact>
      <base>fips-199-moderate</base>
      <selected>fips-199-moderate</selected>
      <adjustment-justification><p>Description</p></adjustment-justification>
    </integrity-impact>
    <availability-impact>
      <base>fips-199-moderate</base>
      <selected>fips-199-moderate</selected>
      <adjustment-justification><p>Description</p></adjustment-justification>
    </availability-impact>
  </information-type>
  <!-- repeat the information-type assembly for each information type -->
  <!-- security-impact-levels -->
</system-information>

```

NOTES:

- Table 2-2 is a subset of Table 15-9. The above OSCAL representation satisfies both.
- For each impact type, if the selected field does not match the base field, the adjustment-justification field is required.



FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name Version #., Date

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2. Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, default to the high-water mark for the Information Types as identified in Table 2-3. Security Impact Level below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	Choose level.
Integrity	Choose level.
Availability	Choose level.

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 2-4. Baseline Security Configuration that follows.

Table 2-4. Baseline Security Configuration

Enter Information System Abbreviation Security Categorization	Choose level
---	--------------

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

FedRAMP 010001100100010101000100010100100100000101000110101010000010011110101
Controlled Unclassified Information

4.9. Security Objectives Categorization (FIPS 199)

Representation

```
<system-characteristics>
  <!-- cut -->
  <security-sensitivity-level>moderate</security-sensitivity-level>
  <!-- system-information -->

  <security-impact-level>
    <security-objective-confidentiality>fips-199-moderate
      </security-objective-confidentiality>

    <security-objective-integrity>fips-199-moderate</security-objective-integrity>
    <security-objective-availability>fips-199-moderate

    </security-objective-availability>
  </security-impact-level>
  <!-- status -->
</system-characteristics>
```

NIST Accepted Values
Valid security sensitivity values:

- low
- moderate
- high

NIST Accepted Values
Valid security objective values:

- fips-199-low
- fips-199-moderate
- fips-199-high

XPath Queries

System Sensitivity Level:
`/*/system-characteristics/security-sensitivity-level`

Security Objective: Confidentiality:
`/*/system-characteristics/security-impact-level/security-objective-confidentiality`

Security Objective: Integrity:
`/*/system-characteristics/security-impact-level/security-objective-integrity`

Security Objective: Availability:
`/*/system-characteristics/security-impact-level/security-objective-availability`

NOTES:

- The security-sensitivity-level field in the OSCAL file satisfies both Table 2-1 and 2-4.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

2.3. Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

At the time of writing, the NIST OSCAL syntax validation tools have a typo for @name="identity-assurance-level", and are instead expecting "identiy-assurance-level"

This section will be updated when the typo is addressed by NIST.

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

Controlled Unclassified Information

4.10. Digital Identity Determination

The digital identity level identified in Section 2.3 is the same as the level in Attachment 3. Both are identified with the same single piece of information, which is a `prop` field with the name "security-eauth-level".

This is a FedRAMP extension, thus requires the `ns` flag set to "fedramp".

Currently, FedRAMP prescribes an overall eAuth level, and does not require individual IAL, AAL, and FAL designations. The overall eAuth level is all that is required; however, the FedRAMP extensions include separate prop statements for each of these three levels to allow for possible future use.

Representation

```
<system-characteristics>
  <prop name="security-eauth-level" class="security-eauth"
        ns="https://fedramp.gov/ns/oscal">2</prop>
  <!-- Attachment 3, Digital Identity Worksheet -->
  <prop name="identity-assurance-level">2</prop>
  <prop name="authenticator-assurance-level">2</prop>
  <prop name="federation-assurance-level">2</prop>
</system-characteristics>
```

FedRAMP Extensions

prop:

- name="security-eauth-level"
ns="https://fedramp.gov/ns/oscal"

NIST Accepted Values

Valid eAuth values:

- 1 for low
- 2 for moderate
- 3 for high

XPath Queries

Digital Identity Level:

```
/*system-characteristics/prop[@name="security-eauth-level"]
  [@ns='https://fedramp.gov/ns/oscal']
```

Identity Assurance Level:

```
/*system-characteristics/prop[@name="identity-assurance-level"]
```

Authenticator Assurance Level:

```
/*system-characteristics/prop[@name="authenticator-assurance-level"]
```

Federation Assurance Level:

```
/*system-characteristics/prop[@name="federation-assurance-level"]
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE															
CSP Name Information System Name	Version #., Date														
<h3>3. INFORMATION SYSTEM OWNER</h3> <p>The following individual is identified as the system owner or functional proponent/advocate for this system.</p> <table border="1"> <thead> <tr> <th colspan="2">Information System Owner Information</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> <tr> <td>Company / Organization</td> <td><Enter Company/Organization></td> </tr> <tr> <td>Address</td> <td><Enter Address, City, State and Zip></td> </tr> <tr> <td>Phone Number</td> <td><555-555-5555></td> </tr> <tr> <td>Email Address</td> <td><Enter email address></td> </tr> </tbody> </table>		Information System Owner Information		Name	<Enter Name>	Title	<Enter Title>	Company / Organization	<Enter Company/Organization>	Address	<Enter Address, City, State and Zip>	Phone Number	<555-555-5555>	Email Address	<Enter email address>
Information System Owner Information															
Name	<Enter Name>														
Title	<Enter Title>														
Company / Organization	<Enter Company/Organization>														
Address	<Enter Address, City, State and Zip>														
Phone Number	<555-555-5555>														
Email Address	<Enter email address>														

FedRAMP 01000110010001000101010001000100000101000110101010000010011110101

Controlled Unclassified Information

4.11. Information System Owner

Representation
<pre> <metadata> <!-- cut --> <role id="system-owner"> <title>Information System Owner</title> <desc>The individual within the CSP who is ultimately accountable for everything related to this system.</desc> </role> <!-- cut --> <party id="person-1"> <person> <person-name>Name of Person 1</person-name> <org-id>csp</org-id> <address> <addr-line></addr-line> <city>City</city> <state>ST</state> <postal-code>12345</postal-code> <country>US</country> </address> <email>name@org.domain</email> <phone></phone> <prop name="title" ns="https://fedramp.gov/ns/oscal">Job Title</prop> </person> </party> <!-- cut --> <responsible-party role-id="system-owner"> <party-id>person-1</party-id> </responsible-party> </metadata> </pre>
XPath Queries
<p>System Owner's Name: <code>/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="system-owner"]/ party-id]]/person/person-name</code></p> <p>NOTE: Replace "person-name" with "org-name", "email" or "phone" above as needed.</p> <p>System Owner's Address: <code>/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="system-owner"]/ party-id]]/person/address/addr-line</code></p> <p>NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.</p> <p>System Owner's Title: <code>/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="system-owner"]/ party-id]]/person/prop[@name='title'][@ns='https://fedramp.gov/ns/oscal']</code></p> <p>Company/Organization: <code>/*/metadata/party[@id=(/*/metadata/party[@id=(/*/metadata/ responsible-party[@role-id="system-owner"]/party-id)[1]]/ person/org-id)]/org/org-name</code></p>

NOTE:

- If no country is provided, FedRAMP tools will assume a US address.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

4. AUTHORIZING OFFICIALS

Instruction: The Authorizing Official is determined by the authorization.

JAB P-ATO: FedRAMP, JAB, as comprised of member rep Administration (GSA), Department of Defense (DoD) and Agency Authority to Operate (ATO): Agency Authorizing

Delete this and all other instructions from your final version.

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the *Insert AO information as instructed above.*

FedRAMP JAB P-ATO Authorization Representation

```
<metadata>
  <!-- cut -->
  <role id="authorizing-official">
    <title>Authorizing Official</title>
    <desc>The individual or individuals who must grant this system an authorization to operate.</desc>
  </role>
  <!-- cut -->
  <party id="fedramp-jab">
    <org>
      <org-name>Federal Risk and Authorization Management Program: Joint Authorization Board</org-name>
      <short-name>FedRAMP JAB</short-name>
    </org>
  </party>
  <!-- cut -->
  <responsible-party role-id="authorizing-official">
    <party-id>fedramp-jab</party-id>
  </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
  <!-- description -->
  <prop name="authorization-type" ns="https://fedramp.gov/ns/oscal">fedramp-jab</prop>
  <!-- annotation -->
</system-characteristics>
```

JAB XPath Queries

Authorizing Official's Name:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official"]]/party-id]]/org/short-name`

Controlled Unclassified Information

4.12. Authorizing Officials

FedRAMP Agency Authorization Representation

```
<metadata>
  <!-- cut -->
  <role id="authorizing-official">
    <title>Authorizing Official</title>
    <desc>The individual or individuals who must grant this system an authorization to operate.</desc>
  </role>
  <!-- cut -->
  <party id="person-6">
    <person>
      <person-name>Name of Person 1</person-name>
      <org-name>A Four Letter Agency</org-name>
      <address>
        <addr-line></addr-line>
        <city></city>
        <state></state>
        <postal-code></postal-code>
        <country>us</country>
      </address>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Job Title</prop>
    </person>
  </party>
  <!-- cut -->
  <responsible-party role-id=" authorizing-official ">
    <party-id>person-6</party-id>
  </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
  <!-- description -->
  <prop name="authorization-type" ns="https://fedramp.gov/ns/oscal">fedramp-agency</prop>
  <!-- annotation -->
</system-characteristics>
```

NIST-Defined Identifier

- Required Role ID:
- authorizing-official

Authorization Type XPath Query

FedRAMP Authorization Type:
`/*/system-characteristics/prop[@name="authorization-type"][@ns="https://fedramp.gov/ns/oscal"]`

FedRAMP Agency and LI-SaaS XPath Queries

Authorizing Official's Name:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official"]]/party-id]]/person/person-name`

Authorizing Official's Title:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official"]]/party-id]]/person/prop[@name='title'][@ns='https://fedramp.gov/ns/oscal']`

Authorizing Official's Agency:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official"]]/party-id]]/person/org-name`

NOTE:

- if the authorization-type field is "fedramp-jab", the responsible-party/party-id field must be "fedramp-jab".

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																																							
CSP Name Information System Name	Version #., Date																																						
5. OTHER DESIGNATED CONTACTS																																							
<p><i>Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.</i></p> <p><i>Delete this and all other instructions from your final version of this document.</i></p>																																							
<p>The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.</p> <table border="1"> <thead> <tr> <th colspan="2"><i>Table 5-1. Information System Management Point of Contact</i></th> </tr> <tr> <th colspan="2">Information System Management Point of Contact</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> <tr> <td>Company / Organization</td> <td><Enter Company/Organization></td> </tr> <tr> <td>Address</td> <td><Enter Address, City, State and Zip></td> </tr> <tr> <td>Phone Number</td> <td><555-555-5555></td> </tr> <tr> <td>Email Address</td> <td><Enter email address></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2"><i>Table 5-2. Information System Technical Point of Contact</i></th> </tr> <tr> <th colspan="2">Information System Technical Point of Contact</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> <tr> <td>Company / Organization</td> <td><Enter Company/Organization></td> </tr> <tr> <td>Address</td> <td><Enter Address, City, State and Zip></td> </tr> <tr> <td>Phone Number</td> <td><555-555-5555> See Next Page</td> </tr> <tr> <td>Email Address</td> <td><Enter email address></td> </tr> </tbody> </table> <p><i>Instruction: Add more tables as needed.</i></p> <p><i>Delete this and all other instructions from your final version of this document.</i></p> <table border="1"> <thead> <tr> <th colspan="2">Point of Contact</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> </tbody> </table>		<i>Table 5-1. Information System Management Point of Contact</i>		Information System Management Point of Contact		Name	<Enter Name>	Title	<Enter Title>	Company / Organization	<Enter Company/Organization>	Address	<Enter Address, City, State and Zip>	Phone Number	<555-555-5555>	Email Address	<Enter email address>	<i>Table 5-2. Information System Technical Point of Contact</i>		Information System Technical Point of Contact		Name	<Enter Name>	Title	<Enter Title>	Company / Organization	<Enter Company/Organization>	Address	<Enter Address, City, State and Zip>	Phone Number	<555-555-5555> See Next Page	Email Address	<Enter email address>	Point of Contact		Name	<Enter Name>	Title	<Enter Title>
<i>Table 5-1. Information System Management Point of Contact</i>																																							
Information System Management Point of Contact																																							
Name	<Enter Name>																																						
Title	<Enter Title>																																						
Company / Organization	<Enter Company/Organization>																																						
Address	<Enter Address, City, State and Zip>																																						
Phone Number	<555-555-5555>																																						
Email Address	<Enter email address>																																						
<i>Table 5-2. Information System Technical Point of Contact</i>																																							
Information System Technical Point of Contact																																							
Name	<Enter Name>																																						
Title	<Enter Title>																																						
Company / Organization	<Enter Company/Organization>																																						
Address	<Enter Address, City, State and Zip>																																						
Phone Number	<555-555-5555> See Next Page																																						
Email Address	<Enter email address>																																						
Point of Contact																																							
Name	<Enter Name>																																						
Title	<Enter Title>																																						

FedRAMP 01000110010001010001000101000100000101000110101010000010011110101

Controlled Unclassified Information

4.13. Other Designated Contacts: Information System Management

Table 5-1 Representation

```

<metadata>
  <!-- cut -->
  <role id="system-poc-management">
    <title>Information System Management Point of Contact (POC)</title>
    <desc>The highest level manager who responsible for system operation on behalf of the System Owner.</desc>
  </role>
  <!-- cut -->
  <party id="person-5">
    <person>
      <person-name>Name 5</person-name>
      <org-name>csp</org-name>
      <address>
        <addr-line>Address Line</addr-line>
        <city>City</city>
        <state>ST</state>
        <postal-code>00000</postal-code>
        <country>US</country>
      </address>
      <email>name@org.domain</email>
      <phone></phone>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Individual's Title</prop>
    </person>
  </party>
  <!-- cut -->
  <responsible-party role-id="system-poc-management">
    <party-id>person-5</party-id>
  </responsible-party>
</metadata>

```

NIST Defined Identifiers

Required Role ID's:

- system-poc-management
- system-poc-technical

FedRAMP Extension

Person's Title:

- prop name="title" ns="https://fedramp.gov/ns/oscal"

XPath Queries

Information System Management POC Name:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="system-poc-management"]]/party-id]]/person/person-name`

NOTE: Replace "person-name" with "email" or "phone" above as needed.

Information System Management POC Title:

`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="system-poc-management"]]/party-id]]/person/prop[@name='title'][@ns="https://fedramp.gov/ns/oscal"]`

Information System Management POC Address Line:

`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="system-poc-management"]]/party-id]]/person/address/addr-line`

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																																			
CSP Name Information System Name	Version #., Date																																		
<h2>5. OTHER DESIGNATED CONTACTS</h2> <p><i>Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.</i></p> <p><i>Delete this and all other instructions from your final version of this document.</i></p>																																			
<p>The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.</p> <p><i>Table 5-1. Information System Management Point of Contact</i></p> <table border="1"> <thead> <tr> <th colspan="2">Information System Management Point of Contact</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> <tr> <td>Company / Organization</td> <td><Enter Company/Organization></td> </tr> <tr> <td>Address</td> <td><Enter Address, City, State and Zip></td> </tr> <tr> <td>Phone Number</td> <td><555-555-5555></td> </tr> <tr> <td>Email Address</td> <td><Enter email address></td> </tr> </tbody> </table> <p><i>Table 5-2. Information System Technical Point of Contact</i></p> <table border="1"> <thead> <tr> <th colspan="2">Information System Technical Point of Contact</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> <tr> <td>Company / Organization</td> <td><Enter Company/Organization></td> </tr> <tr> <td>Address</td> <td><Enter Address, City, State and Zip></td> </tr> <tr> <td>Phone Number</td> <td><555-555-5555></td> </tr> <tr> <td>Email Address</td> <td><Enter email address></td> </tr> </tbody> </table> <p><i>Instruction: Add more tables as needed.</i></p> <p><i>Delete this and all other instructions from your final version of this document.</i></p> <table border="1"> <thead> <tr> <th colspan="2">Point of Contact</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><Enter Name></td> </tr> <tr> <td>Title</td> <td><Enter Title></td> </tr> </tbody> </table>		Information System Management Point of Contact		Name	<Enter Name>	Title	<Enter Title>	Company / Organization	<Enter Company/Organization>	Address	<Enter Address, City, State and Zip>	Phone Number	<555-555-5555>	Email Address	<Enter email address>	Information System Technical Point of Contact		Name	<Enter Name>	Title	<Enter Title>	Company / Organization	<Enter Company/Organization>	Address	<Enter Address, City, State and Zip>	Phone Number	<555-555-5555>	Email Address	<Enter email address>	Point of Contact		Name	<Enter Name>	Title	<Enter Title>
Information System Management Point of Contact																																			
Name	<Enter Name>																																		
Title	<Enter Title>																																		
Company / Organization	<Enter Company/Organization>																																		
Address	<Enter Address, City, State and Zip>																																		
Phone Number	<555-555-5555>																																		
Email Address	<Enter email address>																																		
Information System Technical Point of Contact																																			
Name	<Enter Name>																																		
Title	<Enter Title>																																		
Company / Organization	<Enter Company/Organization>																																		
Address	<Enter Address, City, State and Zip>																																		
Phone Number	<555-555-5555>																																		
Email Address	<Enter email address>																																		
Point of Contact																																			
Name	<Enter Name>																																		
Title	<Enter Title>																																		

FedRAMP 01000110010001010001000101000100000101000110101010000010011110101

Controlled Unclassified Information

4.14. Other Designated Contacts: Information System Technical

Table 5-2 Representation

```

<metadata>
  <!-- cut -->
  </role>
  <role id="system-poc-technical">
    <title>Information System Technical Point of Contact</title>
    <desc>The individual leading the technical operation of the system.</desc>
  </role>
  <role id="system-poc-other">
    <title>Other Information System Point of Contact</title>
  </role>
  <party id="person-7">
    <person>
      <person-name>Name 7</person-name>
      <org-name>csp</org-name>
      <address>
        <!-- cut -->
      </address>
      <email>name@org.domain</email>
      <phone></phone>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Individual's Title</prop>
    </person>
  </party>
  <!-- repeat party assembly for each person -->
  <!-- cut -->
  <responsible-party role-id="system-poc-technical">
    <party-id>person-7</party-id>
  </responsible-party>
  <responsible-party role-id="system-poc-other">
    <party-id>person-8</party-id>
    <party-id>person-9</party-id>
  </responsible-party>
</metadata>

```

NIST-Defined Identifiers

Required Role ID:

- system-poc-technical
- system-poc-other

FedRAMP Extension

Person's Title:

- prop name="title" ns="https://fedramp.gov/ns/oscal"

XPath Queries

Information System Technical POC Name:

```
(/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id=
  "system-poc-technical"]/party-id]]/person/person-name) [1]
```

NOTE: Replace "person-name" with "email" or "phone" above as needed.

Information System Technical POC Title:

```
(/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id=
  "system-poc-technical"]/party-id]]/person/prop[@name='title']
  [@ns="https://fedramp.gov/ns/oscal"]) [1]
```

Information System Technical POC Address Line:

```
(/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id=
  "system-poc-technical"]/party-id]]/person/address/addr-line) [1]
```

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

NOTE: For each additional technical POC, replace the "[1]" with "[2]", "[3]", and so on.

4.15. Assignment of Security Responsibility: ISSO

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Next Page

Table 6-1 Representation

```

<metadata>
  <!-- cut -->
  <role id="information-system-security-officer">
    <title>System Information System Security Officer (or Equivalent)</title>
    <desc>The individual accountable for the security posture of the system
          on behalf of the system owner.</desc>
  </role>
  <!-- cut -->
  <party id="person-10">
    <person>
      <person-name>Name 10</person-name>
      <org-name>CSP Name</org-name>
      <address>
        <addr-line>Address Line</addr-line>
        <city>City</city>
        <state>ST</state>
        <postal-code>00000</postal-code>
        <country>US</country>
      </address>
      <email>name@org.domain</email>
      <phone></phone>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Individual's Title</prop>
    </person>
  </party>
  <!-- cut -->
  <responsible-party role-id="information-system-security-officer">
    <party-id>person-10</party-id>
  </responsible-party>
</metadata>

```

NIST-Defined Identifier

Required Role ID:

- information-system-security-officer

FedRAMP Extension

Person's Title:

- prop name="title"

ns="https://fedramp.gov/ns/oscal"

XPath Queries

ISSO POC Name:

```
/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id=
  "information-system-security-officer"]/party-id]]/person/person-name
```

NOTE: Replace "person-name" with "org-name", "email", or "phone" above as needed.

ISSO POC Title:

```
/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id=
  "information-system-security-officer"]/party-id]]/person/prop
  [@name='title'][@ns="https://fedramp.gov/ns/oscal"]
```

ISSO POC Address Line:

```
/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id=
  "information-system-security-officer"]/party-id]]/person/address/addr-line
```

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

4.16. Assignment of Security Responsibility: AO POC

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Previous Page

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 6-2 Representation

```

<metadata>
  <!-- cut -->
  <role id="authorizing-official-poc">
    <title>Authorizing Official's Point of Contact</title>
    <desc>The individual representing the authorizing official.</desc>
  </role>
  <!-- cut -->
  <party id="person-011">
    <person>
      <person-name>Name 11</person-name>
      <org-name>Agency Name</org-name>
      <address>
        <addr-line>Address Line</addr-line>
        <city>City</city>
        <state>ST</state>
        <postal-code>00000</postal-code>
        <country>US</country>
      </address>
      <email>name@org.domain</email>
      <phone></phone>
      <prop name="title" ns="https://fedramp.gov/ns/oscal">Individual's Title</prop>
    </person>
  </party>
  <!-- cut -->
  <responsible-party role-id="authorizing-official-poc">
    <party-id>person-011</party-id>
  </responsible-party>
</metadata>

```

XPath Queries

AO POC Name:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official-poc"]]/party-id]]/person/person-name`

NOTE: Replace "person-name" with "email" or "phone" above as needed.

AO POC Title:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official-poc"]]/party-id]]/person/prop[@name='title'][@ns="https://fedramp.gov/ns/oscal"]`

AO POC Address Line:
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="authorizing-official-poc"]]/party-id]]/person/address/addr-line`

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

NIST-Defined Identifier

Required Role ID:

- authorizing-official-poc

FedRAMP Extension

Person's Title:

- prop name="title"
ns="https://fedramp.gov/ns/oscal"

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE
CSP Name | Information System Name Version #., Date

7. INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the life-cycle phase shown in Table 7-1. System Status that follows. (Only operational systems can be granted an ATO).

Table 7-1. System Status

System Status		
<input type="checkbox"/>	Operational	The system is operating and in production.
<input type="checkbox"/>	Under Development	The system is being designed, developed, or implemented
<input type="checkbox"/>	Major Modification	The system is undergoing a major change, development, or transition.
<input type="checkbox"/>	Other	Explain: Click here to enter text.

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

Delete this and all other instructions from your final version of this document.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FedRAMP 010001100100010101000100010100100100000101000110101010000010011110101
Controlled Unclassified Information

4.17. Information System Operational Status

Representation

```
<system-characteristics>
  <!-- cut -->

  <!-- security-impact-level -->
  <status state="operational">
    <remarks><p>Remarks are required if status/state is "other". Optional otherwise.</p></remarks>
  </status>
  <!-- leveraged-authorization -->

  <!-- cut -->
</system-characteristics>
```

NIST Accepted Values
Valid state values:

- **operational**
- **under-development**
- **under-major-modification**
- **disposition**
- **other**

XPath Queries

System's Operational Status:
`/*/system-characteristics/status/@state`

The number of paragraphs in the Operational Status Remarks:
`count(/*/system-characteristics/status/remarks/p[1])`

Remarks on System's Operational Status:
`/*/system-characteristics/status/remarks`

NOTE:

- If the status is "other", the `remarks` field is required. Otherwise it is optional.
- While `under-development`, and `disposition` are valid OSCAL values, systems with either of these operational status values are not eligible for a FedRAMP Authorization.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name Version #., Date

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1. Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
<input type="checkbox"/>	Software as a Service (SaaS)	Major Application
<input type="checkbox"/>	Platform as a Service (PaaS)	Major Application
<input type="checkbox"/>	Infrastructure as a Service (IaaS)	General Support System
<input type="checkbox"/>	Other	Explain: Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101
Controlled Unclassified Information

4.18. Cloud Service Models

Representation

```
<system-characteristics>
  <!-- cut -->

  <!-- prop -->
  <annotation name="cloud-service-model" value="saas">
    <remarks>
      <p>Remarks are required if service model is "other". Optional otherwise.</p>
    </remarks>
  </annotation>
  <!-- link or date authorized -->

  <!-- cut -->
</system-characteristics>
```

NIST Accepted Values
Valid Service Model values:

- saas
- paas
- iaas
- other

XPath Queries

```
Service Model:
/*/system-characteristics/annotation[@name="cloud-service-model"]/@value

Remarks on System's Service Model:
/*/system-characteristics/annotation[@name="cloud-service-model"]//remarks
```

NOTE:

- If the service model is "other", the `remarks` field is required. Otherwise it is optional.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name Version #., Date

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2. Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table 8-2. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
<input type="checkbox"/>	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
<input type="checkbox"/>	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
<input type="checkbox"/>	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
<input type="checkbox"/>	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FedRAMP 010001100100010101000100010100100100000101000110101010000010011110101

Controlled Unclassified Information

4.19. Cloud Deployment Models

Representation

```
<system-characteristics>
  <!-- cut -->

  <!-- prop -->
  <annotation name="cloud-deployment-model" value="public">
    <remarks>
      <p>Remarks are required if deployment model is "hybrid". Optional otherwise.</p>
    </remarks>
  </annotation>
  <!-- link or date authorized -->
```

NIST Accepted Values

Valid Service Model values:

- public-cloud
- private-cloud
- community-cloud
- government-only-cloud
- hybrid-cloud
- other

XPath Queries

Deployment Model:
`/*[system-characteristics/annotation[@name="cloud-deployment-model"]]/@value`

Remarks on System's Deployment Model:
`/*[system-characteristics/annotation[@name="cloud-deployment-model"]]/remarks`

NOTE:

- If the deployment model is "hybrid", the remarks field is required. Otherwise it is optional.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name Version #., Date

8.3. Leveraged Authorizations

Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher level layer represented by this SSP plans to leverage a lower layer's Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write "None" in the first column of the table that follows. Add as many rows as necessary in the table that follows.

Delete this and all other instructions from your final version of this document.

The Enter Information System Abbreviation Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Enter Information System Abbreviation are listed in Table 8-3. Leveraged Authorizations that follows.

Table 8-3. Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
<Enter Leveraged information system name1>	<Enter service provider owner1>	<Date>
<Enter Leveraged information system name2>	<Enter service provider owner2>	<Date>
<Enter Leveraged information system name3>	<Enter service provider owner3>	<Date>

The remarks field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

At the time of writing, the NIST OSCAL syntax validation tools require the leveraged-authorization @name attribute, and limits the value to NCName type, which is unintentionally limiting. This section will be updated when the issue is closed by NIST as tracked [HERE](#).

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101
Controlled Unclassified Information

4.20. Leveraged Authorizations

Representation

```

<metadata>
  <!-- role -->
  <party id="eip">
    <org>
      <org-name>Example IaaS Provider</org-name>
      <short-name>E.I.P.</short-name>
      <remarks>
        <p>Underlying service provider. Leveraged Authorization.</p>
      </remarks>
    </org>
  </party>
  <!-- responsible-party -->
</metadata>
<!-- cut -->
<system-characteristics>
  <!-- status -->
  <leveraged-authorization id="lva-1" name="NCName">
    <annotation name="system-name" id="leveraged-01-name"
      ns="https://fedramp.gov/ns/oscal" value="MegaIaaS">
      <remarks><p>Remarks about this system</p></remarks>
    </annotation>
    <party-id>eip</party-id>
    <date-authorized>2018-11-27</date-authorized>
    <remarks><p>Overall notes about the inheritance of controls from this
system</p></remarks>
  </leveraged-authorization>
  <!-- Repeat leveraged-authorization assembly for each leveraged authorization -->
  <!-- authorization-boundary -->
</system-characteristics>

```

FedRAMP Extension annotation

```
(ns="https://fedramp.gov/ns/oscal"):
  • name="system-name"
```

XPath Queries

Leveraged Authorization System Name:
`/*/system-characteristics/leveraged-authorization[1]/annotation[@name="system-name"] [@ns="https://fedramp.gov/ns/oscal"]/value`

Leveraged Authorization Remarks:
`/*/system-characteristics/leveraged-authorization[1]/annotation[@name="system-name"] [@ns="https://fedramp.gov/ns/oscal"]/remarks`

Leveraged Service Provider Owner:
`/*/metadata/party[@id=/*/system-characteristics/leveraged-authorization[1]/party-id]/org/org-name`

Date Granted:
`/*/system-characteristics/leveraged-authorization[1]/date-authorized`

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- The `id` for leveraged-authorization is required by FedRAMP, even though it is optional in the OSCAL syntax. The `id` will be used by each control that inherits from this system.
- If more than one leveraged authorization exists for the system, repeat the entire assembly for each leveraged authorization. Currently this is not typical and should be discussed in advance with the FedRAMP PMO.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name

Version #., Date

9.1. System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system.

Delete this and all other instructions from your final version of this document.

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

Controlled Unclassified Information

4.21. System Function or Purpose

Representation

```
<system-characteristics>
  <!-- system-name, system-name-short -->
  <description>
    <p>Describe the purpose and functions of this system here.</p>
  </description>
  <!-- prop, annotation, link, date-authorized -->
</system-characteristics>
```

XPath Query

System Function or Purpose: First paragraph in description
`/*/system-characteristics/description`

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name Version #., Date

9.2. Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system's Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].

Additional FedRAMP Requirements and Guidance:

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents > FedRAMP Authorization Boundary Guidance <https://www.fedramp.gov/documents/>

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1. Authorization Boundary Diagram below.

In OSCAL, the link field's href flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via back-matter\resource assemblies. This means the href flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. /*/back-matter/resource[@id='diagram-id']

The description fields are *Markup multiline* and the caption field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.22. Authorization Boundary Diagram

The OSCAL approach to this type of diagram is to treat the image data as either a linked or base64-encoded resource in the back-matter section of the OSCAL file, then use a reference to the diagram within the body of the OSCAL file.

Representation

```
<system-characteristics>
  <!-- leveraged-authorization -->
  <authorization-boundary>
    <description>
      <p>A holistic, top-level explanation of the FedRAMP authorization boundary.</p>
    </description>
    <diagram id="sys-boundary-1">
      <description><p>A diagram-specific explanation.</p></description>
      <link href="#diag-boundary-1" rel="diagram" />
      <caption>Authorization Boundary Diagram</caption>
    </diagram>
    <!-- repeat diagram assembly for each additional boundary diagram -->
  </authorization-boundary>
  <!-- network-architecture -->
</system-characteristics>

<!-- cut -->

<back-matter>
  <!-- citation -->
  <resource id="diag-boundary-1">
    <desc>The primary authorization boundary diagram.</desc>
    <base64>00000000</base64>
  </resource>
</back-matter>
```

FedRAMP-Defined Identifiers

Diagram ID:

- sys-boundary-1

Resource ID:

- diag-boundary-1

Replace 1 with a number (2, 3, etc.) as needed.
There should always be a -1 in the SSP.

XPath Queries

Overall Description:

/*/system-characteristics/authorization-boundary/description

Count the Number of Diagrams (There should be at least 1):

count(/*/system-characteristics/authorization-boundary/diagram)

Link to First Diagram:

/*/system-characteristics/authorization-boundary/diagram[1]/link/@href

Replace "[1]" with "[2]", "[3]", etc.

If the diagram link points to a resource within the OSCAL file:

/*/back-matter/resource[@id="diag-boundary-1"]/base64

OR:

/*/back-matter/resource[@id="diag-boundary-1"]/rlink/@href

Diagram-specific Description:

/*/system-characteristics/authorization-boundary/diagram[@id="sys-boundary-1"]/description

NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the authorization boundary diagram to be embedded (base64).

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name Version #., Date

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

NIST Accepted Values

annotation:

- name="type"
 - **Valid:** internal, external, general-public
- name="privilege-type"
 - **Valid:** privileged, non-privileged, no-logical-access

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

See Next Page

FedRAMP 010001100100010101000100010100100100000101000110101010000010011110101

Controlled Unclassified Information

4.23. Personnel Roles and Privileges

Representation

```

<metadata>
  <role id="admin-unix">
    <title>Unix Administrator</title>
    <desc>This is a sample role.</desc>
  </role>
</metadata>
<!-- import -->
<!-- system characteristics -->
<system-implementation>
  <!-- prop -->
  <user id="sys-role-1">
    <title>Unix System Administrator</title>
    <prop name="sensitivity" ns="https://fedramp.gov/ns/oscal">limited</prop>
    <annotation name="type" value="external" />
    <annotation name="privilege-level" value="no-logical-access" />
    <role-id>admin-unix</role-id>
    <authorized-privilege name="Full administrative access (root)">
      <function-performed>Add/remove users and hardware</function-performed>
      <function-performed>install and configure software</function-performed>
      <function-performed>OS updates, patches and hotfixes</function-performed>
      <function-performed>perform backups</function-performed>
    </authorized-privilege>
    <!-- for each user repeat authorized-privilege assembly for each privilege -->
  </user>
  <!-- repeat user assembly for each row in Table 9-1 -->
</system-implementation >
```

FedRAMP Extension & Accepted Values

- ```
prop (ns="https://fedramp.gov/ns/oscal"):
```
- name="sensitivity-level"
    - **Valid:** high-risk, severe, moderate, limited, not-applicable

### XPath Queries

Number of entries in the role table:  
`count(/system-implementation/user)`

Role:  
`/*/system-implementation/user[1]/title`

Internal or External:  
`/*/system-implementation/user[1]/annotation[@name="type"]/@value`

Privileged, Non-Privileged, or No Logical Access:  
`/*/system-implementation/user[1]/annotation[@name="privilege-level"]/@value`

Sensitivity Level:  
`/*/system-implementation/user[1]/prop[@name="sensitivity"][@ns="https://fedramp.gov/ns/oscal"]`

Authorized Privileges:  
`/*/system-implementation/user[1]/authorized-privilege/@name[1]`

Functions Performed:  
`/*/system-implementation/user[1]/authorized-privilege[1]/function-performed[1]`

`count(/system-implementation/user[1]/authorized-privilege[1]/function-performed)`

Replace "[1]" with "[2]", "[3]", etc.

### NOTE:

- FedRAMP prefers the `authorized-privilege` field be repeated within a user assembly if there is more than one, but will accept all `authorized-privileges` in one field during the early stages of OSCAL adoption.
- FedRAMP prefers separate `function-performed` fields for each function performed but will accept all functions in one field during the early stages of OSCAL adoption.

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name Version #., Date

---

### 9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

*Instruction: For an External User, write "Not Applicable" in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)*

*This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.*

*Delete this and all other instructions from your final version of this document.*

*Table 9-1. Personnel Roles and Privileges*

| Role                      | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges             | Functions Performed                                                                                              |
|---------------------------|----------------------|-----------------------------------------------------------------|-------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------|
| UNIX System Administrator | Internal             | P<br><b>See Previous Page</b>                                   | Moderate          | Full administrative access (root) | Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups |
| Client Administrator      | External             | NP                                                              | N/A               | Portal administration             | Add/remote client users. Create, modify and delete client applications                                           |
| Program Director          | Internal             | NLA                                                             | Limited           | N/A                               | Reviews, approves and enforces policy                                                                            |
|                           | Choose an item.      | Choose an item.                                                 | Choose an item.   |                                   |                                                                                                                  |
|                           | Choose an item.      | Choose an item.                                                 | Choose an item.   |                                   |                                                                                                                  |
|                           | Choose an item.      | Choose an item.                                                 | Choose an item.   |                                   |                                                                                                                  |
|                           | Choose an item.      | Choose an item.                                                 | Choose an item.   |                                   |                                                                                                                  |

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

Controlled Unclassified Information

## 4.24. Number of Users

**Representation**

```
<system-implementation>
 <prop name="users-internal" ns="https://fedramp.gov/ns/oscal">22</prop>
 <prop name="users-external" ns="https://fedramp.gov/ns/oscal">110</prop>
 <prop name="users-internal-future" ns="https://fedramp.gov/ns/oscal">25</prop>
 <prop name="users-external-future" ns="https://fedramp.gov/ns/oscal">200</prop>
</system-implementation>
```

**FedRAMP Extensions**

```
prop (ns="https://fedramp.gov/ns/oscal"):
 • name="users-internal"
 • name="users-external"
 • name="users-internal-future"
 • name="users-external-future"
```

**XPath Queries**

Number of current internal users:

```
/*/system-implementation/prop[@name="users-internal"]
[@ns="https://fedramp.gov/ns/oscal"]
```

Number of current external users:

```
/*/system-implementation/prop[@name="users-external"]
[@ns="https://fedramp.gov/ns/oscal"]
```

Number of future internal users (1 year):

```
/*/system-implementation/prop[@name="users-internal-future"]
[@ns="https://fedramp.gov/ns/oscal"]
```

Number of future external users (1 year):

```
/*/system-implementation/prop[@name="users-external-future"]
[@ns="https://fedramp.gov/ns/oscal"]
```

-

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name Version #., Date

---

## 9.4. Network Architecture

*Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.*

*Delete this and all other instructions from your final version of this document.*

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9-2. Network Diagram mapping the data flow between components.

The following Figure 9-2. Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.



In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter\resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/back-matter/resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

## 4.25. Network Architecture Diagram(s)

### Representation

```
<system-characteristics>
 <!-- authorization-boundary -->
 <network-architecture>
 <description>
 <p>A holistic, top-level explanation of the system's network.</p>
 </description>
 <diagram id=" sys-network-1">
 <description><p>A diagram-specific explanation.</p></description>
 <link href="#diag-network-1" rel="diagram" />
 <caption>Network Diagram</caption>
 </diagram>
 <!-- repeat diagram assembly for each additional network diagram -->
 </network-architecture>
 <!-- data-flow -->
</system-characteristics>

<!-- cut -->

<back-matter>
 <!-- citation -->
 <resource id="diag-network-1">
 <desc>The primary network diagram.</desc>
 <rlink href=".//diagram.jpg" media-type="image/jpeg"/>
 </resource>
</back-matter>
```

### FedRAMP-Defined Identifiers

#### Diagram ID:

- sys-network-1

#### Resource ID:

- diag-network-1

Replace 1 with a number (2, 3, etc.) as needed. There should always be a -1 in a SSP.

### XPath Queries

**Overall Description:**  
`/*/system-characteristics/network-architecture/description`

**Count the Number of Diagrams (There should be at least 1):**  
`count(/*/system-characteristics/network-architecture/diagram)`

**Link to First Diagram:**

`/*/system-characteristics/network-architecture/diagram[1]/link/@href`

Replace "[1]" with "[2]", "[3]", etc.

If the diagram link points to a resource within the OSCAL file:  
`/*/back-matter/resource[@id="diag-network-1"]/base64`

OR:

`/*/back-matter/resource[@id="diag-network-1"]/rlink/@href`

**First Diagram Description:**

`/*/system-characteristics/network-architecture/diagram[@id="sys-network-1"]/description`

### NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the network architecture diagrams to be embedded (base64).

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name Version #., Date

---

### 10.1. Data Flow

*Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.*

*Delete this and all other instructions from your final version of this document.*

The data flow in and out of the system boundaries is represented in Figure 10-1. Data Flow Diagram, below.



**Figure 10-1. Data Flow Diagram**

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter\resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/back-matter/resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

## 4.26. Data Flow Diagrams

### Representation

```
<system-characteristics>
 <!-- network-architecture -->
 <data-flow>
 <description>
 <p>A holistic, top-level explanation of the system's data flows.</p>
 </description>
 <diagram id="sys-dataflow-1">
 <description><p>A diagram-specific explanation.</p></description>
 <link href="#diag-dataflow-1" rel="diagram" />
 <caption>Data Flow Diagram</caption>
 </diagram>
 <!-- repeat diagram assembly for each additional data flow diagram -->
 </data-flow>
 <!-- network-architecture -->
</system-characteristics>

<!-- cut -->

<back-matter>
 <!-- citation -->
 <resource id="diag-dataflow-1">
 <desc>The primary data flow diagram.</desc>
 <base64>0000<!-- base64 cut -->0000</base64>
 </resource>
</back-matter>
```

### FedRAMP-Defined Identifiers

#### Diagram ID:

- sys-dataflow-**1**

#### Resource ID:

- diag-dataflow-**1**

Replace **1** with a number (2, 3, etc.) as needed. There should always be a -1 in a SSP.

### XPath Queries

#### Overall Description:

```
/*/system-characteristics/data-flow/description
```

Count the Number of Diagrams (There should be at least 1):  
`count(/*/system-characteristics/data-flow/diagram)`

#### Link to First Diagram:

```
/*/system-characteristics/data-flow/diagram[1]/link/@href
```

Replace "[1]" with "[2]", "[3]", etc.

#### If the diagram link points to a resource within the OSCAL file:

```
/*/back-matter/resource[@id="diag-dataflow-1"]/base64
```

OR:

```
/*/back-matter/resource[@id="diag-dataflow-1"]/rlink/@href
```

#### First Diagram Description:

```
/*/system-characteristics/data-flow/diagram[@id="sys-dataflow-1"]/description
```

### NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the data flow diagrams to be embedded (base64).

## 10.2. Ports, Protocols and Services

The Table 10-1. Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

*Instruction: In the column labeled "Used By" please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled "Purpose" indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.*

*Delete this and all other instructions from your final version of this document.*

Table 10-1. Ports, Protocols and Services

Ports (TCP/UDP)*	Protocols	Services	Purpose	Used By
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>

\* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

At the time of writing, the NIST OSCAL syntax validation tools treat the service @name attribute as and NCName datatype, instead of a string datatype. NIST is investigating. This section will be updated when the issue is closed by NIST as tracked [HERE](#).

## 4.27. Ports, Protocols and Services

### Representation

```

<system-implementation>
 <!-- component -->
 <service id="svc-1" name="ServiceName">
 <prop name="title" ns="https://fedramp.gov/ns/oscal">[SAMPLE] Service Name</prop>
 <prop name="used-by" ns="https://fedramp.gov/ns/oscal">What uses this service?</prop>
 <protocol name="http">
 <port-range start="80" end="80" transport="TCP"/>
 </protocol>
 <protocol name="https">
 <port-range start="443" end="443" transport="TCP"/>
 </protocol>
 <purpose>Describe the purpose of this service</purpose>
 </service>
 <!-- Repeat the service assembly for each row in Table 10-1 -->
 <!-- interconnection, system-inventory -->
</system-implementation>

```

### FedRAMP Extensions

prop (ns="https://fedramp.gov/ns/oscal"):

- name="title"
- name="used-by"

### XPath Queries

Number of entries in the Ports, Protocols and Services table:  
`count(//*[@system-implementation/service])`

Number of protocols specified (1st service):  
`count(//*[@system-implementation/service[1]/protocol])`

Number of port ranges specified:  
`count(//*[@system-implementation/service[1]/protocol[1]/port-range])`

Ports: Start (1st service, 1st protocol, 1st port range):  
`//*[@system-implementation/service[1]/protocol[1]/port-range[1]/@start]`

Ports: End (1st service, 1st protocol, 1st port range):  
`//*[@system-implementation/service[1]/protocol[1]/port-range[1]/@end]`

Ports: Transport (1st service, 1st protocol, 1st port range):  
`//*[@system-implementation/service[1]/protocol[1]/port-range[1]/@transport]`

Protocol (1st service, 1st protocol):  
`//*[@system-implementation/service[1]/protocol[1]/@name]`

Service (1st service):  
`//*[@system-implementation/service[1]/prop[@name="title"][@ns="https://fedramp.gov/ns/oscal"]]`  
OR  
`//*[@system-implementation/service[1]/@name]`

Purpose (1st service):  
`//*[@system-implementation/service[1]/purpose]`

Used By (1st service):  
`//*[@system-implementation/service[1]/prop[@name="used-by"][@ns="https://fedramp.gov/ns/oscal"]]`

**FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE**

CSP Name | Information System Name Version # Date

## II. SYSTEM INTERCONNECTIONS

**Instruction:** List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security, indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13-3 CA-3 Authorized Connections.

**Additional FedRAMP Requirements and Guidance:**

**Guidance:** See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents > FedRAMP Authorization Boundary Guidance <https://www.fedramp.gov/documents/>

Delete this and all other instructions from your final version of this document.

Table 11-1 System Interconnections below is consistent with Table 13-3 CA-3 Authorized Connections.

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

The **remarks** fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

**Table 13-3. CA-3 Authorized Connections**

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

## 4.28. System Interconnections and Authorized Connections (Representation)

Table 11-1 and Table 13-3 are closely related and modeled together in OSCAL.

### Representation

```

<metadata>
 <!-- oscal-version, prop -->
 <role id="isa-poc-remote">
 <title>Remote System POC</title>
 <desc>Role of person who signed the ICA.</desc>
 </role>
 <!-- repeat role assembly for each ICA -->
 <party id="ica-1">
 <person>
 <person-name>Remote POC's Name</person-name>
 <org-name>[SAMPLE]Remote Org Name</org-name>
 <email>person@ica.org.example</email>
 <phone>202-555-1212</phone>
 </person>
 </party>
 <!-- repeat party assembly for each ICA -->
</metadata>
<!-- import-profile, system-characteristics -->
<interconnection id="ica-1">
 <remote-system-name>[EXAMPLE]Authorized Connection System Name</remote-system-name>
 <prop name="service-processor" ns="https://fedramp.gov/ns/oscal">Telco Name</prop>
 <prop name="ip-address-local" ns="https://fedramp.gov/ns/oscal">10.1.1.1</prop>
 <prop name="ip-address-remote" ns="https://fedramp.gov/ns/oscal">10.2.2.2</prop>
 <prop name="direction" ns="https://fedramp.gov/ns/oscal">incoming-outgoing</prop>
 <prop name="information" ns="https://fedramp.gov/ns/oscal">string</prop>
 <prop name="port" ns="https://fedramp.gov/ns/oscal">string</prop>
 <prop name="circuit" ns="https://fedramp.gov/ns/oscal">string</prop>
 <annotation name="connection-security" ns="https://fedramp.gov/ns/oscal">
 value="ipsec"
 <!-- remarks -->
 <remarks><p>If "other", remarks are required. Optional otherwise.</p></remarks>
 </annotation>
 <link href="#cit-isa-1" rel="agreement" />
 <responsible-party role-id="isa-poc-remote">
 <party-id>ica-1</party-id>
 </responsible-party>
 <remarks><p>Optional notes about this interconnection</p></remarks>
</interconnection>
<!-- repeat interconnection assembly for each ICA -->
<!-- control-implementation -->
<back-matter>
 <citation id="cit-isa-1">
 <title>[SAMPLE]Interconnection Security Agreement Title</title>
 <prop name="publication" ns="https://fedramp.gov/ns/oscal">Document Version</prop>
 </citation>
 <!-- repeat citation assembly for each ICA -->
 <!-- resource -->
<back-matter>

```

### XPath Queries

SEE NEXT PAGE

### FedRAMP Extensions & Accepted Values

**prop**

(ns="https://fedramp.gov/ns/oscal"):

- name="service-processor"
- name="ip-address-local"
- name="ip-address-remote"
- name="direction"
  - **Valid:** incoming, outgoing, incoming-outgoing
- name="information"
- name="port"
- name="circuit"

**annotation**

(ns="https://fedramp.gov/ns/oscal"):

- name="connection-security"
  - **Valid:** ipsec, vpn, ssl, certificate, secure-file-transfer, other

### NIST-Defined Identifier

Required Role ID:

- isa-poc-remote

### FedRAMP Extension

**prop**

(ns="https://fedramp.gov/ns/oscal"):

- name="publication"

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE  
CSP Name | Information System Name Version # Date

## II. SYSTEM INTERCONNECTIONS

**Instruction:** List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security, indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13-3 CA-3 Authorized Connections.

**Additional FedRAMP Requirements and Guidance:**

**Guidance:** See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents > FedRAMP Authorization Boundary Guidance <https://www.fedramp.gov/documents/>

Delete this and all other instructions from your final version of this document.

Table 11-1 System Interconnections below is consistent with Table 13-3 CA-3 Authorized Connections.

**Table 11-1. System Interconnections**

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

The remarks fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

**Table 13-3. CA-3 Authorized Connections**

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

## 4.29. System Interconnections and Authorized Connections (Queries)

### XPath Queries

Replace "[1]" with "[2]", "[3]", etc.

(11-1) Service Processor (SP):  
`/*/system-implementation/interconnection[1]/prop[@name="service-processor"][@ns="https://fedramp.gov/ns/oscal"]`

(11-1) IP Address and Interface:  
`/*/system-implementation/interconnection[1]/prop[@name="ip-address-local"][@ns="https://fedramp.gov/ns/oscal"]`

(11-1) External Organization Name ...:  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]//org-name`  
AND IP Address of System:  
`/*/system-implementation/interconnection[1]/prop[@name="ip-address-remote"][@ns="https://fedramp.gov/ns/oscal"]`

(11-1) External Point of Contact ...:  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]//person-name`

AND Phone Number:  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]//phone`

(11-1) Connection Security:  
`/*/system-implementation/interconnection[1]/annotation[@name="connection-security"][@ns="https://fedramp.gov/ns/oscal"]/@value`

(11-1) Connection Security - Remark (required if "other"):  
`/*/system-implementation/interconnection[1]/annotation[@name="connection-security"][@ns="https://fedramp.gov/ns/oscal"]/remarks`

(11-1) Data Direction:  
`/*/system-implementation/interconnection[1]/prop[@name="direction"][@ns="https://fedramp.gov/ns/oscal"]`

(11-1) Information Being Transmitted:  
`/*/system-implementation/interconnection[1]/prop[@name="information"][@ns="https://fedramp.gov/ns/oscal"]`

(11-1) Port or Circuit Numbers:  
`/*/system-implementation/interconnection[1]/prop[@name="port"][@ns="https://fedramp.gov/ns/oscal"]`  
OR:  
`/*/system-implementation/interconnection[1]/prop[@name="circuit"][@ns="https://fedramp.gov/ns/oscal"]`

(13-3) Authorized Connections Information System Name:  
`/*/system-implementation/interconnection[1]/remote-system-name`

(13-3) Name of Organization CSP Name System Connects To [same as (11-1) External Org Name]:  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]//org-name`

(13-3) Role of Person Who Signed Connection Agreement  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]/person/prop[@name="title"][@ns="https://fedramp.gov/ns/oscal"]`

(13-3) Name of Person Who Signed Connection Agreement [same as (11-1)]  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]//person-name`

(11-1) POC Phone Number:  
`/*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-id]//phone`

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name      Version #., Date

---

## 12. LAWS, REGULATIONS, STANDARDS AND GUIDANCE

### 12.1. Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: [Templates](#).

Table 12-1. Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.

*Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional laws and regulations that it must follow, please specify "N/A" in the table.*

*Delete this and all other instructions from your final version of this document.*

**Table 12-1. Information System Name Laws and Regulations**

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

---

### 12.2. Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: [Templates](#)

Table 12-2. Information System Name Standards and Guidance includes in this section any additional standards and guidance specific to Information System Name.

*Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional standards or guidance that it must follow, please specify "N/A" in the table.*

*Delete this and all other instructions from your final version of this document.*

**Table 12-2. Information System Name Standards and Guidance**

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

---

FedRAMP 0100011001000101010001000100010000010100110101010000010011110101

## 4.30. Laws, Regulations, Standards and Guidance

**Representation**

```

<back-matter>
 <citation id="cit-1">
 <target>https://domain.example/path/to/document.pdf</target>
 <title>[SAMPLE]Name or Title of Document</title>
 <prop name="type" ns="https://fedramp.gov/ns/oscal">law</prop>
 <prop name="ref-id" ns="https://fedramp.gov/ns/oscal">Identification
 Number</prop>
 <prop name="publication" ns="https://fedramp.gov/ns/oscal">Document Date</prop>
 </citation>
 <citation id="cit-2">
 <target>https://domain.example/path/to/document.pdf</target>
 <title>[SAMPLE]Name or Title of Document</title>
 <prop name="type" ns="https://fedramp.gov/ns/oscal">guidance</prop>
 <prop name="ref-id" ns="https://fedramp.gov/ns/oscal">Identification
 Number</prop>
 <prop name="publication" ns="https://fedramp.gov/ns/oscal">Document Date</prop>
 </citation>
 <!-- repeat citation assembly for each law, regulation, standard or guidance -->
 <!-- resource -->
</back-matter>

```

**FedRAMP Extensions & Accepted Values**

prop (ns="https://fedramp.gov/ns/oscal"):

- name="type"
  - **Valid:** law, regulation, standard, guidance
- name="ref-id"
- name="publication"

**XPath Queries**

Replace "[1]" with "[2]", "[3]", etc.

Number of Laws and Regulations:  
`count(//*[@back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])`

Laws and Regulations - Identification Number:  
`(//*[@back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])[1]/../prop[@name="ref-
id"][@ns="https://fedramp.gov/ns/oscal"])`

Laws and Regulations - Title:  
`(//*[@back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])[1]/../title`

Laws and Regulations - Date:  
`(//*[@back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])[1]/
..//prop[@name="publication"][@ns="https://fedramp.gov/ns/oscal"])`

Laws and Regulations - Link:  
`(//*[@back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])[1]/../target`

For Standards and Guidance replace "law" with "standard" and "regulation" with "guidance" in the above queries.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE		Version #., Date						
CSP Name   Information System Name								
<b>13.1. Access Control (AC)</b>								
AC-1 Access Control Policy and Parameter Assignments (H)								
<p>The organization:</p> <p><b>NIST control requirement statements</b></p> <p>(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <p>(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and</p> <p><b>FedRAMP additional requirement statements</b></p> <p>(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and</p> <p><b>NIST parameter labels</b></p> <p>(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and</p> <p><b>FedRAMP parameter constraints</b></p> <p>(b) Reviews and updates the current:</p> <p>(1) Access control policy [FedRAMP Assignment: at least annually]; and</p> <p>(2) Access control procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].</p>								
AC-1	Control Summary Information							
<b>Responsible Roles</b>								
Responsible Role:								
Parameter AC-1(a):								
Parameter AC-1(b)(1):								
Parameter AC-1(b)(2):								
Implementation Status (check all that apply):								
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable								
<b>Implementation Status</b>								
Control Origination (check all that apply):								
<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)								
<b>Control Origination</b>								
Implementation Description, including:								
AC-1 What is the solution and how is it implemented?								
<table border="1"> <tr> <td>Part a</td> <td>FIPS 140-2 Validation References</td> </tr> <tr> <td>Part b1</td> <td>Cited Document References</td> </tr> <tr> <td>Part b2</td> <td>Customer Responsibility Matrix</td> </tr> </table>			Part a	FIPS 140-2 Validation References	Part b1	Cited Document References	Part b2	Customer Responsibility Matrix
Part a	FIPS 140-2 Validation References							
Part b1	Cited Document References							
Part b2	Customer Responsibility Matrix							
FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101								

## 5. SECURITY CONTROLS

This section describes the modeling security control information in an OSCAL-based FedRAMP SSP. To ensure consistent processing, FedRAMP imposes specific requirements on the use of OSCAL for control implementation information.

The modeling of controls is addressed on the following pages in four separate sections as follows:

- **Control Definitions**
- **Responsible Roles and Parameter Assignments**
- **Implementation Status**
- **Control Origination**
- **Implementation Descriptions**

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name      Version #., Date

---

**AC-8 System Use Notification (L) (M) (H)**

The information system:

- (a) Displays to users [Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
  - (1) Users are accessing a U.S. Government information system;
  - (2) Information system usage may be monitored, recorded, and subject to audit;
  - (3) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
  - (4) Use of the information system indicates consent to monitoring and recording;
- (b) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
- (c) For publicly accessible systems:
  - (1) Displays system use information [Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)], before granting further access;
  - (2) Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
  - (3) Includes a description of the authorized uses of the system.

**AC-8 Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

**Requirement:** The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

**Guidance:** If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

**Requirement:** If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

---

FedRAMP 0100011001000101010001000100010000010100110101010000010011110101

## 5.1. Control Definitions

All control definition information is imported from the appropriate FedRAMP profile (baseline). This includes the original NIST control definition and parameter labels, as well as any FedRAMP requirement additions, and parameter constraints.

Interpreting and presenting profile content is beyond the scope of this document. Please refer to the NIST OSCAL Profile and Catalog schema references for more information:

- [Profile Model](#)
- [Catalog Reference](#)

Only the control implementation information is present within an OSCAL-based SSP. Each control in the FedRAMP baseline must have a corresponding implemented-requirement assembly in the control-implementation assembly.

### Representation

```
<!-- metadata -->
<import-profile href="https://path/to/xml/FedRAMP_MODERATE-baseline_profile.xml"/>
<!-- system-characteristics -->
<!-- system-implementation -->
<control-implementation>
 <description>
 <p>FedRAMP SSP Template Section 13</p>
 <p>Description field required by OSCAL.</p>
 <p>FedRAMP requires no specific content here.</p>
 </description>
 <implemented-requirement control-id="ac-1">
 <!-- Control content cut - See next pages for detail -->
 </implemented-requirement>
 <implemented-requirement control-id="ac-2" />
 <!-- Control content cut - See next pages for detail -->
 </implemented-requirement>
 <implemented-requirement control-id="ac-2.1" />
 <!-- Control content cut - See next pages for detail -->
 </implemented-requirement>
 <!-- cut -->
</control-implementation>
<!-- back-matter -->
```

### XPath Queries

URI to Profile:  
/\*/import-profile/@href

Replace "ac-1" with target control ID.

CSP's Control Implementation Information  
/\*/control-implementation/implemented-requirement[@control-id="ac-1"]

### NOTE:

- FedRAMP tools check to ensure there is one implemented-requirement assembly for each control identified in the FedRAMP baseline.
- The OSCAL syntax requires the `description` field at the start of the `control-implementation` assembly. FedRAMP requires no specific information here at this time.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																																																			
CSP Name   Information System Name	Version #., Date																																																		
<table border="1"> <thead> <tr> <th>AC-2</th> <th>Control Summary Information</th> </tr> </thead> <tbody> <tr> <td>Responsible Role:</td> <td></td> </tr> <tr> <td>Parameter AC-2(a):</td> <td></td> </tr> <tr> <td>Parameter AC-2(e):</td> <td></td> </tr> <tr> <td>Parameter AC-2(f):</td> <td></td> </tr> <tr> <td>Parameter AC-2(j):</td> <td></td> </tr> <tr> <td colspan="2">Implementation Status (check all that apply):</td> </tr> <tr> <td colspan="2"> <input type="checkbox"/> Implemented  <input type="checkbox"/> Partially implemented  <input type="checkbox"/> Planned  <input type="checkbox"/> Alternative implementation  <input type="checkbox"/> Not applicable         </td> </tr> <tr> <td colspan="2">Control Origination (check all that apply):</td> </tr> <tr> <td colspan="2"> <input type="checkbox"/> Service Provider Corporate  <input type="checkbox"/> Service Provider System Specific  <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)  <input type="checkbox"/> Configured by Customer (Customer System Specific)  <input type="checkbox"/> Provided by Customer (Customer System Specific)  <input type="checkbox"/> Shared (Service Provider and Customer Responsibility)  <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization         </td> </tr> <tr> <td colspan="2"> <a href="#">See Next Pages</a> <small>enter text. , Date of Authorization</small> </td> </tr> <tr> <td colspan="2"> <table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table> </td> </tr> <tr> <td colspan="2"> <small>FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101</small> </td> </tr> </tbody> </table>		AC-2	Control Summary Information	Responsible Role:		Parameter AC-2(a):		Parameter AC-2(e):		Parameter AC-2(f):		Parameter AC-2(j):		Implementation Status (check all that apply):		<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable		Control Origination (check all that apply):		<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization		<a href="#">See Next Pages</a> <small>enter text. , Date of Authorization</small>		<table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table>		AC-2 What is the solution and how is it implemented?		Part a		Part b		Part c		Part d		Part e		Part f		Part g		Part h		Part i		Part j		Part k		<small>FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101</small>	
AC-2	Control Summary Information																																																		
Responsible Role:																																																			
Parameter AC-2(a):																																																			
Parameter AC-2(e):																																																			
Parameter AC-2(f):																																																			
Parameter AC-2(j):																																																			
Implementation Status (check all that apply):																																																			
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable																																																			
Control Origination (check all that apply):																																																			
<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization																																																			
<a href="#">See Next Pages</a> <small>enter text. , Date of Authorization</small>																																																			
<table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table>		AC-2 What is the solution and how is it implemented?		Part a		Part b		Part c		Part d		Part e		Part f		Part g		Part h		Part i		Part j		Part k																											
AC-2 What is the solution and how is it implemented?																																																			
Part a																																																			
Part b																																																			
Part c																																																			
Part d																																																			
Part e																																																			
Part f																																																			
Part g																																																			
Part h																																																			
Part i																																																			
Part j																																																			
Part k																																																			
<small>FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101</small>																																																			

## 5.2. Responsible Roles and Parameter Assignments

Every control must have at least one `responsible-role` defined. There must be a separate `responsible-role` assembly for each responsible role. OSCAL requires the specified `role-id` to be valid in the defined list of roles in the metadata.

FedRAMP further requires the specified `role-id` must also have been referenced in the `system-implementation/user` assembly. This equates to the FedRAMP requirement of all responsible roles appearing in the Personnel Roles and Privileges table.

There must be one `set-parameter` statement for each of the control's parameters, as specified in the FedRAMP baseline. The only exception to this is with nested parameters. Some Select parameters contain an assignment parameter within them, such as appears in AC-7 (b). In these instances, only the final selected value must be provided. The nested assignment parameter may be ignored.

### Representation

```

<metadata>
 <role id="admin-unix">
 <title>Unix Administrator</title>
 <desc>This is a sample role.</desc>
 </role>
</metadata>

<!-- Fragment: -->
<system-implementation>
 <user id="sys-role-1">
 <role-id>admin-unix</role-id>
 </user>
</system-implementation >

<!-- system-implementation -->
<control-implementation>
 <implemented-requirement control-id="ac-2">
 <!-- cut -->
 <responsible-role role-id="admin-unix" />
 <set-param param-id="ac-1_prm_a">
 <value>System Manager, System Architect, ISSO</value>
 </set-param>
 <!-- cut -->
 </control-implementation>
<!-- back-matter -->

```

### XPath Queries

Replace "ac-2" with target control ID.

Number of specified Responsible Roles:  
`count(//*[@control-implementation/implemented-requirement[@control-id="ac-2"]]/responsible-role)`

Replace "[1]" with "[2]", "[3]", etc.

Responsible Role:  
`/*/metadata/role[@id=/*/control-implementation/implemented-requirement[@control-id="ac-1"]]/responsible-role[1]/@role-id]/title`

Check for existence in Personnel Roles and Privileges (Should return a number > 0)  
`count(//*[@system-implementation/user/role-id[string(.)=/*/control-implementation/implemented-requirement[@control-id="ac-2"]]/responsible-role/@role-id])`

Parameter Value:  
`/*/control-implementation/implemented-requirement[@control-id="ac-2"]/set-param[@param-id="ac-2_prm_1"]/value`

Replace "ac-2\_prm\_1" with target parameter ID.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																																																					
CSP Name   Information System Name	Version #., Date																																																				
<table border="1"> <thead> <tr> <th>AC-2</th> <th>Control Summary Information</th> </tr> </thead> <tbody> <tr> <td>Responsible Role:</td> <td></td> </tr> <tr> <td>Parameter AC-2(a):</td> <td></td> </tr> <tr> <td>Parameter AC-2(e):</td> <td></td> </tr> <tr> <td>Parameter AC-2(f):</td> <td></td> </tr> <tr> <td>Parameter AC-2(j):</td> <td></td> </tr> <tr> <td colspan="2"> <b>Implementation Status (check all that apply):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Implemented</li> <li><input type="checkbox"/> Partially implemented</li> <li><input type="checkbox"/> Planned</li> <li><input type="checkbox"/> Alternative implementation</li> <li><input type="checkbox"/> Not applicable</li> </ul> </td> </tr> <tr> <td colspan="2"> <b>Control Origination (check all that apply):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Service Provider Corporate</li> <li><input type="checkbox"/> Service Provider System Specific</li> <li><input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)</li> <li><input type="checkbox"/> Configured by Customer (Customer System Specific)</li> <li><input type="checkbox"/> Provided by Customer (Customer System Specific)</li> <li><input type="checkbox"/> Shared (Service Provider and Customer Responsibility)</li> <li><input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a>, Date of Authorization</li> </ul> </td> </tr> <tr> <td colspan="2"> <table border="1"> <thead> <tr> <th colspan="5">AC-2 What is the level of implementation?</th> </tr> </thead> <tbody> <tr> <td>Part a</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part b</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part c</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part d</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part e</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> </td> </tr> <tr> <td colspan="2"> <b>FedRAMP Extensions and Accepted Values</b> <pre> prop (ns="https://fedramp.gov/ns/oscal"):   • name="planned-completion-date" annotation (ns="https://fedramp.gov/ns/oscal"):   • name="implementation-status"     Valid: implemented, partial, planned, alternate, not-applicable </pre> </td> </tr> <tr> <td colspan="2"> <p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p> </td> </tr> </tbody> </table>		AC-2	Control Summary Information	Responsible Role:		Parameter AC-2(a):		Parameter AC-2(e):		Parameter AC-2(f):		Parameter AC-2(j):		<b>Implementation Status (check all that apply):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Implemented</li> <li><input type="checkbox"/> Partially implemented</li> <li><input type="checkbox"/> Planned</li> <li><input type="checkbox"/> Alternative implementation</li> <li><input type="checkbox"/> Not applicable</li> </ul>		<b>Control Origination (check all that apply):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Service Provider Corporate</li> <li><input type="checkbox"/> Service Provider System Specific</li> <li><input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)</li> <li><input type="checkbox"/> Configured by Customer (Customer System Specific)</li> <li><input type="checkbox"/> Provided by Customer (Customer System Specific)</li> <li><input type="checkbox"/> Shared (Service Provider and Customer Responsibility)</li> <li><input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a>, Date of Authorization</li> </ul>		<table border="1"> <thead> <tr> <th colspan="5">AC-2 What is the level of implementation?</th> </tr> </thead> <tbody> <tr> <td>Part a</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part b</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part c</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part d</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part e</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		AC-2 What is the level of implementation?					Part a					Part b					Part c					Part d					Part e					<b>FedRAMP Extensions and Accepted Values</b> <pre> prop (ns="https://fedramp.gov/ns/oscal"):   • name="planned-completion-date" annotation (ns="https://fedramp.gov/ns/oscal"):   • name="implementation-status"     Valid: implemented, partial, planned, alternate, not-applicable </pre>		<p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>	
AC-2	Control Summary Information																																																				
Responsible Role:																																																					
Parameter AC-2(a):																																																					
Parameter AC-2(e):																																																					
Parameter AC-2(f):																																																					
Parameter AC-2(j):																																																					
<b>Implementation Status (check all that apply):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Implemented</li> <li><input type="checkbox"/> Partially implemented</li> <li><input type="checkbox"/> Planned</li> <li><input type="checkbox"/> Alternative implementation</li> <li><input type="checkbox"/> Not applicable</li> </ul>																																																					
<b>Control Origination (check all that apply):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Service Provider Corporate</li> <li><input type="checkbox"/> Service Provider System Specific</li> <li><input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)</li> <li><input type="checkbox"/> Configured by Customer (Customer System Specific)</li> <li><input type="checkbox"/> Provided by Customer (Customer System Specific)</li> <li><input type="checkbox"/> Shared (Service Provider and Customer Responsibility)</li> <li><input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a>, Date of Authorization</li> </ul>																																																					
<table border="1"> <thead> <tr> <th colspan="5">AC-2 What is the level of implementation?</th> </tr> </thead> <tbody> <tr> <td>Part a</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part b</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part c</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part d</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Part e</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		AC-2 What is the level of implementation?					Part a					Part b					Part c					Part d					Part e																										
AC-2 What is the level of implementation?																																																					
Part a																																																					
Part b																																																					
Part c																																																					
Part d																																																					
Part e																																																					
<b>FedRAMP Extensions and Accepted Values</b> <pre> prop (ns="https://fedramp.gov/ns/oscal"):   • name="planned-completion-date" annotation (ns="https://fedramp.gov/ns/oscal"):   • name="implementation-status"     Valid: implemented, partial, planned, alternate, not-applicable </pre>																																																					
<p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>																																																					

### 5.3. Implementation Status

FedRAMP only accepts only one of five values for `implementation-status`: `implemented`, `partial`, `planned`, `alternative`, and `not-applicable`. A control may be marked "partial" and "planned" (using two separate `implementation-status` fields). All other choices are mutually exclusive.

If the `implementation-status` is `partial`, the gap must be explained in the remarks field.

If the `implementation-status` is `planned`, a brief description of the plan to address the gap, including major milestones must be explained in the remarks field. There must also be a prop (`name="planned-completion-date"` `ns="https://fedramp.gov/ns/oscal"`) field containing the intended completion date.

If the `implementation-status` is `alternative`, the alternative implementation must be summarized in the remarks field.

If the `implementation-status` is `not-applicable`, the N/A justification must be provided in the remarks field.

#### Implementation Status Representation

```

<!-- system-implementation -->
<control-implementation>
 <implemented-requirement control-id="ac-1">
 <prop name="planned-completion-date" ns="https://fedramp.gov/ns/oscal">
 2021-01-01Z</prop>
 <annotation name="implementation-status" ns="https://fedramp.gov/ns/oscal" value="implemented" />
 <annotation name="implementation-status" ns="https://fedramp.gov/ns/oscal" value="partial" />
 <remarks><p>Describe the unsatisfied gap.</p></remarks>
 </annotation>
 <annotation name="implementation-status" ns="https://fedramp.gov/ns/oscal" value="planned" />
 <remarks><p>Describe the plan to complete the implementation.</p></remarks>
 </annotation>
 <annotation name="implementation-status" ns="https://fedramp.gov/ns/oscal" value="not-applicable" />
 <remarks><p>Justification for marking control Not Applicable.</p></remarks>
 </annotation>
 </control-implementation>
 <!-- responsible-role -->
 <!-- back-matter -->

```

#### Implementation Status XPath Queries

Implementation Status (may return more than 1 result for a given control):  
`/*control-implementation/implemented-requirement[@control-id="ac-1"]/prop[@name="implementation-status"] [not(@ns)]`

Gap Description (If `implementation-status="partial"`):  
`/*control-implementation/implemented-requirement[@control-id="ac-1"]/annotation[@name="partial"][@ns="https://fedramp.gov/ns/oscal"]/remarks`

Planned Completion Date (If `implementation-status="planned"`):  
`/*control-implementation/implemented-requirement[@control-id="ac-1"]/prop[@name="planned-completion-date"][@ns="https://fedramp.gov/ns/oscal"]`

Plan for Completion (If `implementation-status="planned"`):  
`/*control-implementation/implemented-requirement[@control-id="ac-1"]/annotation[@name="planned"][@ns="https://fedramp.gov/ns/oscal"]/remarks`

Not Applicable (N/A) Justification (If `implementation-status="na"`):  
`/*control-implementation/implemented-requirement[@control-id="ac-1"]/annotation[@name="na"][@ns="https://fedramp.gov/ns/oscal"]/remarks`

Replace  
"ac-1" with  
target  
control-id.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																	
CSP Name   Information System Name	Version #., Date																
<table border="1"> <thead> <tr> <th>AC-2</th> <th>Control Summary Information</th> </tr> </thead> <tbody> <tr> <td>Responsible Role:</td> <td></td> </tr> <tr> <td>Parameter AC-2(a):</td> <td></td> </tr> <tr> <td>Parameter AC-2(e):</td> <td></td> </tr> <tr> <td>Parameter AC-2(f):</td> <td></td> </tr> <tr> <td>Parameter AC-2(j):</td> <td><b>See Previous Pages</b></td> </tr> <tr> <td>Implementation Status (check all that apply):</td> <td> <input type="checkbox"/> Implemented  <input type="checkbox"/> Partially implemented  <input type="checkbox"/> Planned  <input type="checkbox"/> Alternative implementation  <input type="checkbox"/> Not applicable         </td> </tr> <tr> <td>Control Origination (check all that apply):</td> <td> <input type="checkbox"/> Service Provider Corporate  <input type="checkbox"/> Service Provider System Specific  <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)  <input type="checkbox"/> Configured by Customer (Customer System Specific)  <input type="checkbox"/> Provided by Customer (Customer System Specific)  <input type="checkbox"/> Shared (Service Provider and Customer Responsibility)  <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a>, <a href="#">Date of Authorization</a> </td> </tr> </tbody> </table>		AC-2	Control Summary Information	Responsible Role:		Parameter AC-2(a):		Parameter AC-2(e):		Parameter AC-2(f):		Parameter AC-2(j):	<b>See Previous Pages</b>	Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , <a href="#">Date of Authorization</a>
AC-2	Control Summary Information																
Responsible Role:																	
Parameter AC-2(a):																	
Parameter AC-2(e):																	
Parameter AC-2(f):																	
Parameter AC-2(j):	<b>See Previous Pages</b>																
Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable																
Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , <a href="#">Date of Authorization</a>																
<table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr> <td>Part a</td> <td></td> </tr> <tr> <td>Part b</td> <td></td> </tr> <tr> <td>Part c</td> <td></td> </tr> <tr> <td>Part d</td> <td></td> </tr> <tr> <td>Part e</td> <td></td> </tr> <tr> <td>Part f</td> <td></td> </tr> <tr> <td>Part g</td> <td></td> </tr> </tbody> </table>		AC-2 What is the solution and how is it implemented?		Part a		Part b		Part c		Part d		Part e		Part f		Part g	
AC-2 What is the solution and how is it implemented?																	
Part a																	
Part b																	
Part c																	
Part d																	
Part e																	
Part f																	
Part g																	
<b>FedRAMP Extensions and Accepted Values</b> <pre>prop(ns="https://fedramp.gov/ns/oscal"):   • name="leveraged-authorization-id"   annotation(ns="https://fedramp.gov/ns/oscal"):     • name="control-origination"       <b>Valid:</b> sp-corporate, sp-system, customer-configured, customer-provided, inherited       Instead of hybrid, identify multiple control-origination types, each in its own annotation assembly.</pre>																	
<p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>																	

## 5.4. Control Origination

FedRAMP accepts only one of five values for `control-origination`: `sp-corporate`, `sp-system`, `customer-configured`, `customer-provided`, and `inherited`. Hybrid choices are now expressed by identifying more than one control-origination, each in a separate annotation field.

For controls with a control-id ending in "-1", FedRAMP only accepts `sp-corporate`, and `sp-system`.

If the control origination is `inherited`, there must also be a `prop(name="leveraged-authorization" ns="https://fedramp.gov/ns/oscal")` field containing the Leveraged Authorization ID of the appropriate system as it appears in the `/*/system-characteristics/leveraged-authorization` assembly.

### Control Origination Representation

```
<system-characteristics>
 <!-- status -->
 <leveraged-authorization id="lva-1" name="NCName">
 <!-- details cut -- see Leveraged Authorizations Section -->
 </leveraged-authorization>
</system-characteristics>
<!-- system-implementation -->
<control-implementation>
 <implemented-requirement control-id="ac-2">
 <prop name="leveraged-authorization-id" ns="https://fedramp.gov/ns/oscal">
 lva-1</prop>
 <annotation name="control-origination" ns="https://fedramp.gov/ns/oscal" value="sp-corporate" />
 <annotation name="control-origination" ns="https://fedramp.gov/ns/oscal" value="sp-system" />
 <annotation name="control-origination" ns="https://fedramp.gov/ns/oscal" value="customer-configured" />
 <annotation name="control-origination" ns="https://fedramp.gov/ns/oscal" value="inherited" />
 <!-- responsible-role -->
</control-implementation>
<!-- back-matter -->
```

### XPath Queries

Replace "ac-2" with target control-id.

Number of Control Originations:  
`count(/*/control-implementation/implemented-requirement[@control-id="ac-2"])/annotation[@name="control-origination"][@ns="https://fedramp.gov/ns/oscal"])`

Control Origination (could return more than 1 result):  
`/*/control-implementation/implemented-requirement[@control-id="ac-2"]/annotation[@name="control-origination"][@ns="https://fedramp.gov/ns/oscal"] [1]/@value`

Inherited From: System Name (If `control-origination="inherited"`):  
`/*/system-characteristics/leveraged-authorization[@id=/*/control-implementation/implemented-requirement[@control-id="ac-2"]]/prop[@name="leveraged-authorization-id"][@ns="https://fedramp.gov/ns/oscal"]]/annotation[@name="system-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`

Replace "[1]" with "[2]", "[3]", etc.

Inherited From: Authorization Date (If `control-origination="inherited"`):  
`/*/system-characteristics/leveraged-authorization[@id=/*/control-implementation/implemented-requirement[@control-id="ac-2"]]/prop[@name="leveraged-authorization-id"][@ns="https://fedramp.gov/ns/oscal"]]/date-authorized`

<b>Policy and Procedure Statements</b>												
The organization:												
(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:												
<ul style="list-style-type: none"> <li>(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and</li> </ul>												
(b) Reviews and updates the current:												
<ul style="list-style-type: none"> <li>(1) Access control policy [FedRAMP Assignment: at least annually]; and</li> <li>(2) Access control procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].</li> </ul>												
<b>AC-1 What is the solution and how is it implemented?</b>												
<table border="1"> <tr><td>Part a</td></tr> <tr><td>Part b1</td></tr> <tr><td>Part b2</td></tr> </table>		Part a	Part b1	Part b2								
Part a												
Part b1												
Part b2												
<b>Multi-Part Statements</b>												
The organization:												
<ul style="list-style-type: none"> <li>(a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];</li> <li>(b) Assigns account managers for information system accounts;</li> </ul>												
<ul style="list-style-type: none"> <li>cut c, d, e, f, g, h, i</li> <li>(j) Reviews accounts for compliance with account management requirements [FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access]; and</li> <li>(k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.</li> </ul>												
<b>AC-2 What is the solution and how is it implemented?</b>												
<table border="1"> <tr><td>Part a</td></tr> <tr><td>Part b</td></tr> <tr><td>Part c</td></tr> <tr><td>Part d</td></tr> <tr><td>Part e</td></tr> <tr><td>Part f</td></tr> <tr><td>Part g</td></tr> <tr><td>Part h</td></tr> <tr><td>Part i</td></tr> <tr><td>Part j</td></tr> <tr><td>Part k</td></tr> </table>		Part a	Part b	Part c	Part d	Part e	Part f	Part g	Part h	Part i	Part j	Part k
Part a												
Part b												
Part c												
Part d												
Part e												
Part f												
Part g												
Part h												
Part i												
Part j												
Part k												
<b>Single Statement</b>												
The organization employs automated mechanisms to support the management of information system accounts.												
<b>AC-2 (I) What is the solution and how is it implemented?</b>												

## 5.5. Control Implementation Description: Overview

The OSCAL file must contain one implemented-requirement assembly for each part specified in the existing FedRAMP SSP Templates. For most controls and control enhancements in the FedRAMP Baselines based on NIST SP 800-53, Revision 4, this translates as follows:

- Policy and Procedure Statements
- Multi-Part Statements
- Single Statements

### 5.5.1. Policy and Procedure Statements

For each of the -1 controls, such as AC-1, there must be exactly three statements: Part (a), Part (b)(1) and Part (b)(2).

#### Policy and Procedure Representation

```
<!-- system-implementation -->
<control-implementation>
 <!-- cut -->
 <implemented-requirement control-id="ac-1">
 <statement statement-id="ac-1_stmt.a"><!-- cut --></statement>
 <statement statement-id="ac-1_stmt.b.1"><!-- cut --></statement>
 <statement statement-id="ac-1_stmt.b.2"><!-- cut --></statement>
 </control-implementation>
<!-- back-matter -->
```

### 5.5.2. Multi-Part Statements:

If there are outlined parts in the control requirement (a., b., etc.), such as with AC-2, the `statement-id` points to the first-level, lettered statements (`statement-id="ac-2_smt.a"`), and there must be one for each lettered statement. With the exception of Policy and Procedure Statements above, FedRAMP does not currently require responses at the sub-part level.

#### Multi-Part Statement Representation

```
<!-- system-implementation -->
<control-implementation>
 <!-- cut -->
 <implemented-requirement control-id="ac-2">
 <statement statement-id="ac-2_stmt.a"><!-- cut --></statement>
 <statement statement-id="ac-2_stmt.b"><!-- cut --></statement>
 <!-- cut c, d, e, f, g, h, i -->
 <statement statement-id="ac-2_stmt.j"><!-- cut --></statement>
 <statement statement-id="ac-2_stmt.k"><!-- cut --></statement>
 </control-implementation>
<!-- back-matter -->
```

### 5.5.3. Single Statement

If there are no outlined parts in the control requirement (no a, b, etc.), such as with AC-2 (1), the `control-id` points to the top-level statement (`control-id="ac-2.1_smt"`), and there must be exactly one.

#### Single-Statement Representation

```
<!-- system-implementation -->
<control-implementation>
 <!-- cut -->
 <implemented-requirement control-id="ac-2.1">
 <statement statement-id="ac-2.1_stmt"><!-- cut --></statement>
 </control-implementation>
<!-- back-matter -->
```

FedRAMP may change this when NIST SP 800-53 Revision 5 is published in 2020.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																																															
CSP Name   Information System Name	Version #., Date																																														
<table border="1"> <thead> <tr> <th>AC-2</th> <th>Control Summary Information</th> </tr> </thead> <tbody> <tr> <td>Responsible Role:</td> <td></td> </tr> <tr> <td>Parameter AC-2(a):</td> <td></td> </tr> <tr> <td>Parameter AC-2(e):</td> <td></td> </tr> <tr> <td>Parameter AC-2(f):</td> <td></td> </tr> <tr> <td>Parameter AC-2(j):</td> <td></td> </tr> <tr> <td>Implementation Status (check all that apply):</td> <td> <input type="checkbox"/> Implemented  <input type="checkbox"/> Partially implemented  <input type="checkbox"/> Planned  <input type="checkbox"/> Alternative implementation  <input type="checkbox"/> Not applicable         </td> </tr> <tr> <td>Control Origination (check all that apply):</td> <td> <input type="checkbox"/> Service Provider Corporate  <input type="checkbox"/> Service Provider System Specific  <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)  <input type="checkbox"/> Configured by Customer (Customer System Specific)  <input type="checkbox"/> Provided by Customer (Customer System Specific)  <input type="checkbox"/> Shared (Service Provider and Customer Responsibility)  <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a>, Date of Authorization         </td> </tr> <tr> <td colspan="2" style="text-align: center;">See Previous Pages</td> </tr> <tr> <td colspan="2"> <table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table> </td> </tr> <tr> <td colspan="2"> <p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p> </td> </tr> </tbody> </table>		AC-2	Control Summary Information	Responsible Role:		Parameter AC-2(a):		Parameter AC-2(e):		Parameter AC-2(f):		Parameter AC-2(j):		Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization	See Previous Pages		<table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table>		AC-2 What is the solution and how is it implemented?		Part a		Part b		Part c		Part d		Part e		Part f		Part g		Part h		Part i		Part j		Part k		<p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>	
AC-2	Control Summary Information																																														
Responsible Role:																																															
Parameter AC-2(a):																																															
Parameter AC-2(e):																																															
Parameter AC-2(f):																																															
Parameter AC-2(j):																																															
Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable																																														
Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization																																														
See Previous Pages																																															
<table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table>		AC-2 What is the solution and how is it implemented?		Part a		Part b		Part c		Part d		Part e		Part f		Part g		Part h		Part i		Part j		Part k																							
AC-2 What is the solution and how is it implemented?																																															
Part a																																															
Part b																																															
Part c																																															
Part d																																															
Part e																																															
Part f																																															
Part g																																															
Part h																																															
Part i																																															
Part j																																															
Part k																																															
<p>The <b>remarks</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>																																															

## 5.6. Control Implementation Description: Approaches

OSCAL makes two approaches available for control implementation descriptions at the statement level:

- **Flat-File Approach:** Similar to today's FedRAMP SSPs, where the entire control description for each part is kept together, regardless of its implementation point; and
- **Component-Based Approach:** The control description for each part is broken down and described based on its relevant component.

**FedRAMP SSP tools must support both approaches.** FedRAMP prefers the component-based approach, but will accept the flat-file approach to aid existing CSPs who are converting existing MS-Word based FedRAMP SSPs to OSCAL.

With the **flat-file approach**, all of the content in the cell next to *Part a* appears in a single OSCAL file, just as it does in today's FedRAMP SSP templates.

AC-2 What is the solution and how is it implemented?		
Part a	OSCAL description Field	Describes how <i>part a</i> is satisfied by the system at the platform, and web server. Describes what is inherited from the underlying IaaS provider. Describes the customer responsibilities.
Part b	OSCAL description Field	Describes how <i>part b</i> is satisfied by the system at the platform, and web server. Describes what is inherited from the underlying IaaS provider. Describes the customer's responsibilities.

With the complete NIST **component-based approach**, the content in the cell next to *Part a* must be broken down into its individual components and responded to separately.

AC-2 What is the solution and how is it implemented?		
Part a	platform	Describes how <i>part a</i> is satisfied by the platform.
Part b	platform	Describes how <i>part b</i> is satisfied by the platform.
Part a	web-server	Describes how <i>part a</i> is satisfied by the web server
Part a	inherited	Describes what is inherited from the underlying IaaS provider.
Part a	customer	Describes the customer's responsibilities.
Part b	platform	Describes how <i>part b</i> is satisfied by the platform.
Part b	web-server	Describes how <i>part b</i> is satisfied by the web server
Part b	inherited	Describes what is inherited from the underlying IaaS provider.
Part b	customer	Describes the customer's responsibilities.

FedRAMP encourages CSPs to take a limited-component approach, defining one component to represent the system, one to represent the customer, and one to represent each underlying service provider. Each control implementation description should be broken down based on these three components. **See Appendix D: Working with Components for more information.**

A mix of approaches is also acceptable. For example, a CSP may wish to keep the flat-file approach for the Policy and Procedure (-1) controls, but use a component-based approach for technical controls or controls with a customer responsibility.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																			
CSP Name   Information System Name	Version #., Date																		
<b>13.1. Access Control (AC)</b>																			
<b>AC-1 Access Control Policy and Procedures Requirements (H)</b>																			
<p><b>The organization:</b></p> <p>(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ul style="list-style-type: none"> <li>(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and</li> </ul> <p>(b) Reviews and updates the current:</p> <ul style="list-style-type: none"> <li>(1) Access control policy [FedRAMP Assignment: at least annually]; and</li> <li>(2) Access control procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].</li> </ul>																			
<table border="1"> <thead> <tr> <th>AC-1</th> <th>Control Summary Information</th> </tr> </thead> <tbody> <tr> <td>Responsible Role:</td> <td></td> </tr> <tr> <td>Parameter AC-1(a):</td> <td></td> </tr> <tr> <td>Parameter AC-1(b)(1):</td> <td></td> </tr> <tr> <td>Parameter AC-1(b)(2):</td> <td></td> </tr> <tr> <td colspan="2">Implementation Status (check all that apply):</td> </tr> <tr> <td colspan="2"> <input type="checkbox"/> Implemented  <input type="checkbox"/> Partially implemented  <input type="checkbox"/> Planned  <input type="checkbox"/> Alternative implementation  <input type="checkbox"/> Not applicable         </td> </tr> <tr> <td colspan="2">Control Origination (check all that apply):</td> </tr> <tr> <td colspan="2"> <input type="checkbox"/> Service Provider Corporate  <input type="checkbox"/> Service Provider System Specific  <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)         </td> </tr> </tbody> </table> <p style="text-align: center;"><b>See Previous Pages</b></p>		AC-1	Control Summary Information	Responsible Role:		Parameter AC-1(a):		Parameter AC-1(b)(1):		Parameter AC-1(b)(2):		Implementation Status (check all that apply):		<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable		Control Origination (check all that apply):		<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)	
AC-1	Control Summary Information																		
Responsible Role:																			
Parameter AC-1(a):																			
Parameter AC-1(b)(1):																			
Parameter AC-1(b)(2):																			
Implementation Status (check all that apply):																			
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable																			
Control Origination (check all that apply):																			
<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)																			
<table border="1"> <thead> <tr> <th colspan="2">AC-1 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr> <td>Part a</td> <td></td> </tr> <tr> <td>Part b1</td> <td></td> </tr> <tr> <td>Part b2</td> <td></td> </tr> </tbody> </table>		AC-1 What is the solution and how is it implemented?		Part a		Part b1		Part b2											
AC-1 What is the solution and how is it implemented?																			
Part a																			
Part b1																			
Part b2																			
<p>The <b>description</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <i>Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</i>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>																			

### 5.6.1. Flat-File Approach

The flat-file approach enables a CSP to simply represent the content of each cell in the table to the right as an individual part

#### Representation

```
<!-- system-implementation -->
<control-implementation>
 <!-- cut -->
 <implemented-requirement control-id="ac-1">
 <statement statement-id="ac-1_stmt.a">
 <description><p>Implementation Description for Part a.</p></description>
 </statement>
 <statement statement-id="ac-1_stmt.b.1">
 <description><p>Implementation Description for Part b, 1.</p></description>
 </statement>
 <statement statement-id="ac-1_stmt.b.2">
 <description><p>Implementation Description for Part b, 1.</p></description>
 </statement>
 </control-implementation>
 <!-- back-matter -->
```

#### XPath Queries

```
AC-1 What is the solution and how is it implemented?, Part (a):
/*/control-implementation/implemented-requirement[@control-id="ac-1"]/statement
[@statement-id="ac-1_stmt.a"]/description

AC-1 What is the solution and how is it implemented?, Part (b1):
/*/control-implementation/implemented-requirement[@control-id="ac-1"]/statement
[@statement-id="ac-1_stmt.b.1"]/description

AC-1 What is the solution and how is it implemented?, Part (b2):
/*/control-implementation/implemented-requirement[@control-id="ac-1"]/statement
[@statement-id="ac-1_stmt.b.2"]/description
```

#### NOTES:

- All **statement-id** values must be cited as they appear in the NIST SP 800-53, Revision 4 OSCAL catalog: [https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/nist.gov/SP800-53/rev4/xml/NIST\\_SP-800-53\\_rev4\\_catalog.xml](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/nist.gov/SP800-53/rev4/xml/NIST_SP-800-53_rev4_catalog.xml)
- If using the flat-file approach, and the control origination indicates **customer-provided**, or **customer-configured**, the content in the remarks for control-origination must be sufficient to satisfy the customer-responsibility-matrix (CRM).

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE																									
CSP Name   Information System Name	Version #., Date																								
<table border="1"> <thead> <tr> <th>AC-2</th> <th>Control Summary Information</th> </tr> </thead> <tbody> <tr> <td>Responsible Role:</td> <td></td> </tr> <tr> <td>Parameter AC-2(a):</td> <td></td> </tr> <tr> <td>Parameter AC-2(e):</td> <td></td> </tr> <tr> <td>Parameter AC-2(f):</td> <td></td> </tr> <tr> <td>Parameter AC-2(j):</td> <td></td> </tr> <tr> <td>Implementation Status (check all that apply):</td> <td> <input type="checkbox"/> Implemented  <input type="checkbox"/> Partially implemented  <input type="checkbox"/> Planned  <input type="checkbox"/> Alternative implementation  <input type="checkbox"/> Not applicable         </td> </tr> <tr> <td>Control Origination (check all that apply):</td> <td> <input type="checkbox"/> Service Provider Corporate  <input type="checkbox"/> Service Provider System Specific  <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)  <input type="checkbox"/> Configured by Customer (Customer System Specific)  <input type="checkbox"/> Provided by Customer (Customer System Specific)  <input type="checkbox"/> Shared (Service Provider and Customer Responsibility)  <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a>, Date of Authorization         </td> </tr> </tbody> </table>		AC-2	Control Summary Information	Responsible Role:		Parameter AC-2(a):		Parameter AC-2(e):		Parameter AC-2(f):		Parameter AC-2(j):		Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization								
AC-2	Control Summary Information																								
Responsible Role:																									
Parameter AC-2(a):																									
Parameter AC-2(e):																									
Parameter AC-2(f):																									
Parameter AC-2(j):																									
Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable																								
Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization																								
<b>See Previous Pages</b>																									
<table border="1"> <thead> <tr> <th colspan="2">AC-2 What is the solution and how is it implemented?</th> </tr> </thead> <tbody> <tr><td>Part a</td><td></td></tr> <tr><td>Part b</td><td></td></tr> <tr><td>Part c</td><td></td></tr> <tr><td>Part d</td><td></td></tr> <tr><td>Part e</td><td></td></tr> <tr><td>Part f</td><td></td></tr> <tr><td>Part g</td><td></td></tr> <tr><td>Part h</td><td></td></tr> <tr><td>Part i</td><td></td></tr> <tr><td>Part j</td><td></td></tr> <tr><td>Part k</td><td></td></tr> </tbody> </table>		AC-2 What is the solution and how is it implemented?		Part a		Part b		Part c		Part d		Part e		Part f		Part g		Part h		Part i		Part j		Part k	
AC-2 What is the solution and how is it implemented?																									
Part a																									
Part b																									
Part c																									
Part d																									
Part e																									
Part f																									
Part g																									
Part h																									
Part i																									
Part j																									
Part k																									
<p>The <b>description</b> fields are <i>Markup multiline</i>, which enables the text to be formatted. This requires special handling. See <a href="#">Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL</a>, or visit: <a href="https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline">https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline</a></p>																									

### 5.6.2. Component Approach

Within each of the statement assemblies, FedRAMP prefers all responses appear in one of three by-component assemblies as follows:

- **Service Provider Origin** (`component-id="comp-system"`): Describe **how** the cloud service provider is satisfying the control requirement.
- **Inherited** (`component-id="comp-fedramp-authorized-provider-1"`): Describe what is being inherited from a leveraged authorization. If there is more than one leveraged authorization (not typical), be sure to define a component for each underlying system and use the correct component-id here. If this specific statement is inheriting from more than one provider, list each as a separate by-component assembly.
- **Customer Responsibility** (`component-id="comp-customer"`): Describe any customer responsibilities here.

#### Representation

```
<!-- system-implementation -->
<control-implementation>
 <!-- cut -->
 <implemented-requirement control-id="ac-2">
 <statement statement-id="ac-2_stmt.a">
 <description><p>Descriptions appear in by-component section(s)</p></description>
 <!-- Service Provider Responsibility -->
 <by-component component-id="comp-system">
 <description>
 <p>How is the service provider satisfying the control</p>
 </description>
 </by-component>
 <!-- Inherited -->
 <by-component component-id="comp-fedramp-authorized-provider-1">
 <description><p>What is inherited?</p></description>
 </by-component>
 <!-- Customer Responsibility -->
 <by-component component-id="comp-customer">
 <description>
 <p>What must the customer configure or provide?</p>
 <p>This will appear in the Customer Responsibility Matrix.</p>
 </description>
 </by-component>
 </statement>
 <!-- repeat statement assembly for statement part as needed. -->
 </control-implementation>
 <!-- back-matter -->
```

#### XPath Queries

[SEE NEXT PAGE](#)

#### NOTES:

- All `statement-id` values must be cited as they appear in the NIST SP 800-53, Revision 4 OSCAL catalog: [https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/nist.gov/SP800-53/rev4/xml/NIST\\_SP-800-53\\_rev4\\_catalog.xml](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/nist.gov/SP800-53/rev4/xml/NIST_SP-800-53_rev4_catalog.xml)
- Tool vendors should expect to see this component approach expand in the future and may want to design tools with this in mind. Contact the NIST OSCAL Team ([oscal@nist.gov](mailto:oscal@nist.gov)) or the FedRAMP PMO ([info@fedramp.gov](mailto:info@fedramp.gov)) for more information.
- If using the component-based approach, and the control origination indicates `customer-provided`, or `customer-configured` the customer component must be used to capture the customer's responsibility for each part, sufficient to satisfy the customer responsibility matrix.

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name      Version #., Date

---

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply):	<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable
Control Origination (check all that apply):	<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization

**See Previous Pages**

---

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

### 5.6.3. XPath Queries for Control Implementation Descriptions

#### XPath Queries

AC-2 What is the solution and how is it implemented?, Part (a):  
`/*/control-implementation/implemented-requirement[@control-id="ac-2"]/  
statement[@statement-id="ac-2_stmt.a"]/by-component[@component-id="comp-system"]/  
description`

Replace "ac-2" with target control-id.

Description of WHAT is Inherited:  
`/*/control-implementation/implemented-requirement[@control-id="ac-2"]/  
statement[@statement-id="ac-2_stmt.a"]/by-component[@component-id=  
"comp-fedramp-authorized-provider-1"]/description`

Replace "ac-2\_stmt.a" with target control statement-id.

Description of Customer Responsibilities:  
`/*/control-implementation/implemented-requirement[@control-id="ac-2"]/  
statement[@statement-id="ac-2_stmt.a"]/by-component[@component-id="comp-customer"]/  
description`

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name

Version #., Date

---

## 15. ATTACHMENTS

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. *Example* Enter Information System Abbreviation A1 ISPP xx v1.0. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

*Table 15-1. Names of Provided Attachments*

Attachment	File Name	File Extension
Information Security Policies and Procedures	Enter Information System Abbreviation A1 ISPP xx v1.0	.enter extension
User Guide	Enter Information System Abbreviation A2 UG v1.0	.enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA (if needed)	Enter Information System Abbreviation A4 PIA v1.0	.enter extension
Rules of Behavior	Enter Information System Abbreviation A5 ROB v1.0	.enter extension
Information System Contingency Plan	Enter Information System Abbreviation A6 ISCP v1.0	.enter extension
Configuration Management Plan	Enter Information System Abbreviation A7 CMP v1.0	.enter extension
Incident Response Plan	Enter Information System Abbreviation A8 IRP v1.0	.enter extension
CIS Workbook	Enter Information System Abbreviation A9 CIS Workbook v1.0	.enter extension
FIPS 199	Included in Section 15	
Inventory	Enter Information System Abbreviation A13 INV v1.0	.enter extension

---

FedRAMP 01000110010001010100010001010010010000010100110101010000010011110101

## 6. ATTACHMENTS

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The following table describes how each attachment is handled:

ATTACHMENT	MACHINE READABLE	HOW TO HANDLE
Policies and Procedures	No	Attach using the <a href="#">back-matter, resource</a> syntax.  Use <code>resource id="att-policy-1"</code> for policies, and set type to "policy".  Use <code>resource id="att-procedure-1"</code> for procedures, and set type to "procedure".
User Guide	No	Attach using the <a href="#">back-matter, resource</a> syntax.  Use <code>resource id="att-guide-1"</code> for guides, and set type to "guide".
Digital Identity Worksheet	Yes	Incorporated above. See the <i>Digital Identity Determination</i> Section.
Privacy Threshold Analysis (PTA)	Yes	Incorporated into System Information. See the <i>Privacy Impact Assessment</i> Section.
Privacy Impact Assessment (PIA)	No (Future)	Attach using the <a href="#">back-matter, resource</a> syntax. Use <code>resource id="att-pia"</code> . FedRAMP intends to incorporate machine-readable PIA content into the OSCAL-based FedRAMP SSP at a later date.
Rules of Behavior	No	Attach using the <a href="#">back-matter, resource</a> syntax. Use <code>resource id="att-rob"</code> for procedures, and set type to "rob".
Information System Contingency Plan	No	Attach using the <a href="#">back-matter, resource</a> syntax. Use <code>resource id="att-plan-cp"</code> for procedures, and set type to "plan".
Configuration Management Plan	No	Attach using the <a href="#">back-matter, resource</a> syntax. Use <code>resource id="att-plan-cm"</code> for procedures, and set type to "plan".
Incident Response Plan	No	Attach using the <a href="#">back-matter, resource</a> syntax. Use <code>resource id="att-plan-ir"</code> for procedures, and set type to "plan".
CIS Workbook	Yes	This can be generated from the content in the Security Controls section and no longer needs to be maintained separately or attached.
FIPS-199	Yes	Incorporated above. See the <i>Security Objectives Categorization (FIPS-199)</i> Section.
Inventory	Yes	See the <i>System Inventory</i> Section below.

**FEDRAMP SYSTEM SECURITY PLAN (SSP) \_\_\_\_\_ BASELINE TEMPLATE**

CSP Name | Information System Name

Version #., Date

**15. ATTACHMENTS**

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. *Example* Enter Information System Abbreviation A1 ISPP xx v1.0. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

*Table 15-1. Names of Provided Attachments*

Attachment	File Name	File Extension
<b>Information Security Policies and Procedures</b>	Enter Information System Abbreviation A1 ISPP xx v1.0	.enter extension
<b>User Guide</b>	Enter Information System Abbreviation A2 UG v1.0	.enter extension
<b>Digital Identity Worksheet</b>	Included in Section 15	
<b>PTA</b>	Included in Section 15	
<b>PIA (if needed)</b>	Enter Information System Abbreviation A4 PIA v1.0	.enter extension
<b>Rules of Behavior</b>	Enter Information System Abbreviation A5 ROB v1.0	.enter extension
<b>Information System Contingency Plan</b>	Enter Information System Abbreviation A6 ISCP v1.0	.enter extension
<b>Configuration Management Plan</b>	Enter Information System Abbreviation A7 CMP v1.0	.enter extension
<b>Incident Response Plan</b>	Enter Information System Abbreviation A8 IRP v1.0	.enter extension
<b>CIS Workbook</b>	Enter Information System Abbreviation A9 CIS Workbook v1.0	.enter extension
<b>FIPS 199</b>	Included in Section 15	
<b>Inventory</b>	Enter Information System Abbreviation A13 INV v1.0	.enter extension

**6.1. Attachments**

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The following table describes how each attachment is handled:

**Attachment Representation**

```
<!-- cut -->
<back-matter>
 <!-- citation -->
 <resource id="att-policy-1">
 <desc>Policy document</desc>
 <prop name="type" ns="https://fedramp.gov/ns/oscal">policy</prop>
 <prop name="title" ns="https://fedramp.gov/ns/oscal">Document Title</prop>
 <prop name="publication" ns="https://fedramp.gov/ns/oscal">Document Date</prop>
 <prop name="version" ns="https://fedramp.gov/ns/oscal">Document Version</prop>
 <!-- Add rlink with relative path or embed with base64 encoding -->
 <base64>00000000</base64>
 </resource>
 <resource id="att-policy-2" />
 <!-- cut: policies 3 - 13 -->
 <resource id="att-policy-14" />
 <resource id="att-procedure-1" />
 <!-- cut: procedure 2 - 13 -->
 <resource id="att-policy-14" />
 <resource id="att-guide-user" />
 <resource id="att-rob" />
 <resource id="att-plan-cp" />
 <resource id="att-plan-cm" />
 <resource id="att-plan-ir" />
</back-matter>
```

**FedRAMP Extensions & Accepted Values**

```
prop (ns="https://fedramp.gov/ns/oscal"):
 • name="type"
 o Valid: policy, procedure, guide, pia, rob, plan
 • name="title"
 • name="publication"
 • name="version"
```

**XPath Queries**

The Number of Policies Attached:

```
count(//*[@back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]][string(.)="policy"])
```

Attachment (Embedded Base64 encoded):

```
/*/back-matter/resource[@id="att-policy-1"]/base64
```

OR (Relative Link):

```
/*/back-matter/resource[@id="att-policy-1"]/rlink/@href
```

Replace "policy" with "plan", "rob", etc. for each attachment type.

Title of First Policy Document:

```
/*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"] [string(.)="policy"] [1]/..//prop[@name="title"][@ns="https://fedramp.gov/ns/oscal"]
```

## ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](#).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found..**

### Privacy Overview and Point of Contact (POC)

The Table 15-6. Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

**Table 15-6. Information System Name; Privacy POC**

Name	Click here to enter text.
Title	Click here to enter text.
CSP / Organization	Click here to enter text.
Address	Click here to enter text.
Phone Number	Click here to enter text.
Email Address	Click here to enter text.

## 6.2. Privacy Impact Assessment: POC

Much of the Privacy Impact Assessment (PIA) is absorbed into constructs addressed earlier in this document. The Privacy POC is handled the same as other roles. The same is true for the laws and regulations.

### Attachment Representation

```
<!-- cut -->
<metadata>
 <role id="privacy-poc">
 <title>Privacy Official's Point of Contact</title>
 <desc>The individual responsible for the PTA and if necessary the PIA.</desc>
 </role>
 <!-- cut -->
 <party id="person-007">
 <person>
 <person-name>[SAMPLE] Person Name 7</person-name>
 <org-name>CSP Name</org-name>
 <address>
 <addr-line>Suite 0000</addr-line>
 <addr-line>1234 Some Street</addr-line>
 <city>Haven</city>
 <state>ME</state>
 <postal-code>00000</postal-code>
 </address>
 <email>name@org.domain</email>
 <phone>000-000-0000</phone>
 <prop name="title" ns="https://fedramp.gov/ns/oscal">Individual's Title</prop>
 </person>
 </party>
 <!-- cut -->
 <responsible-party role-id="privacy-poc">
 <party-id>person-007</party-id>
 </responsible-party>
</role>
</metadata>
```

### NIST-Defined Identifier

Required Role ID:

- privacy-poc

### XPath Queries

POC Name:  
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="privacy-poc"]]/party-id]]/*/person-name`

POC Org Name:  
`/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="privacy-poc"]]/party-id]]/*/org-name`

NOTE: Replace "org-name" with "phone", "email", "address/addr-line", "address/city", "address/state", or "address/zip" as needed. There may be more than one "addr-line"

## ATTACHMENT 4 PTA/PIA

*This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.*

*Delete this note and all other instructions from your final version of this document.*

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](#).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found..**

Table 1S-7. <Information System Name> Laws and Regulations

Identification Number	Title	Date	Link
Click here to enter text.			
Click here to enter text.			

## 6.3. Privacy Impact Assessment: Laws and Regulations

Much of the Privacy Impact Assessment (PIA) is absorbed into constructs addressed earlier in this document. The Privacy POC is handled the same as other roles. The same is true for the laws and regulations.

### Attachment Representation

```
<!-- cut -->
<back-matter>
 <citation id="cit-2">
 <target>https://domain.example/path/to/document.pdf</target>
 <title>[SAMPLE] Privacy-Related Law Citation</title>
 <prop name="type" ns="https://fedramp.gov/ns/oscal">law</prop>
 <prop name="type" ns="https://fedramp.gov/ns/oscal">pii</prop>
 <prop name="ref-id" ns="https://fedramp.gov/ns/oscal">Identification Number</prop>
 <prop name="publication" ns="https://fedramp.gov/ns/oscal">Publication Date</prop>
 </citation>
</back-matter>
```

### XPath Queries

Number of Privacy Laws and Regulations:

```
count((/*/back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.)="law") or (string(.)="regulation")])../prop[@name="type"]
[@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii"))])
```

Privacy Laws and Regulations - Identification Number:

```
((/*/back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])../prop[@name="type"]
[@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii")))[1]/..prop[@name="ref-id"]
[@ns="https://fedramp.gov/ns/oscal"])
```

Laws and Regulations - Title:

```
((/*/back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])../prop[@name="type"]
[@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii"))][1]/..title
```

Privacy Laws and Regulations - Date:

```
((/*/back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])../prop[@name="type"]
[@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii"))][1]/..
prop[@name="publication"][@ns="https://fedramp.gov/ns/oscal"]
```

Privacy Laws and Regulations - Link:

```
((/*/back-matter/citation/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
[(string(.) = "law") or (string(.)="regulation")])../prop[@name="type"]
[@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii"))][1]/..target
```

Replace "[1]" with "[2]", "[3]", etc.

## ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](#).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found..**

### DESIGNATION

Check one.

- A Privacy Sensitive System
- Not a Privacy Sensitive System (in its current version)

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: [Templates](#).

### QUALIFYING QUESTIONS

- |            |                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Select One | 1. Does the ISA collect, maintain, or share PII in any identifiable form?                                                                      |
| Select One | 2. Does the ISA collect, maintain, or share PII information from or about the public?                                                          |
| Select One | 3. Has a Privacy Impact Assessment ever been performed for the ISA?                                                                            |
| Select One | 4. Is there a Privacy Act System of Records Notice (SORN) for this ISA system?<br>If yes; the SORN identifier and name is: Enter SORN ID/Name. |

If answers to Questions 1-4 are all "No" then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment.

## 6.4. Privacy Impact Assessment: Designation and Qualifying Questions

### Attachment Representation

```
<!-- cut -->
<system-characteristics>
 <system-information>
 <!-- Attachment 4, PTA/PIA Designation -->
 <prop name="privacy-sensitive">yes</prop>
 <!--Does the ISA collect, maintain, or share PII in any identifiable form? -->
 <prop name="pta-1" class="pta" ns="https://fedramp.gov/ns/oscal">yes</prop>
 <!--Does the ISA collect, maintain, share PII info from or about the public? -->
 <prop name="pta-2" class="pta" ns="https://fedramp.gov/ns/oscal">yes</prop>
 <!--Has a Privacy Impact Assessment ever been performed for the ISA? -->
 <prop name="pta-3" class="pta" ns="https://fedramp.gov/ns/oscal">yes</prop>
 <!--Is there a Privacy Act System of Records Notice (SORN) for this ISA system? -->
 <prop name="pta-4" class="pta" ns="https://fedramp.gov/ns/oscal">yes</prop>
 <prop name="sorn-id" class="pta" ns="https://fedramp.gov/ns/oscal">[No SORN
ID]</prop>
 <!-- information-type -->
 </system-information>
</system-characteristics>
```

### FedRAMP Extensions & Accepted Values

- prop (ns="https://fedramp.gov/ns/oscal", class="pta"):
- name="privacy-sensitive"
    - **Valid:** yes, no
  - name="pta-1"
    - **Valid:** yes, no
  - name="sorn-id"

### XPath Queries

```
Privacy Designation (yes = Privacy Sensitive):
/*/system-characteristics/system-information/prop[@name="privacy-sensitive"]

Qualifying Question #1:
/*/system-characteristics/system-information/prop[@name="pta-1"]
[@ns="https://fedramp.gov/ns/oscal"]

Qualifying Question #2:
/*/system-characteristics/system-information/prop[@name="pta-2"]
[@ns="https://fedramp.gov/ns/oscal"]

Qualifying Question #3:
/*/system-characteristics/system-information/prop[@name="pta-3"]
[@ns="https://fedramp.gov/ns/oscal"]

Qualifying Question #4:
/*/system-characteristics/system-information/prop[@name="pta-4"]
[@ns="https://fedramp.gov/ns/oscal"]

Qualifying Question #4:
/*/system-characteristics/system-information/prop[@name="sorn-id"]
[@ns="https://fedramp.gov/ns/oscal"]
```

## ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](#).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	VIRTUAL	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

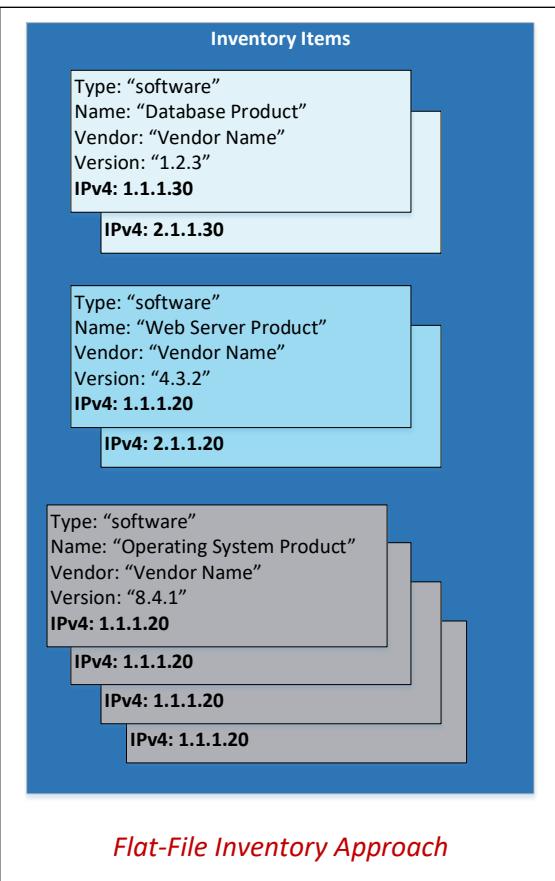
Software and Database Inventories			Any Inventory					
Software/Database Vendor	Software/Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/Network ID	System Administrator/Owner	Application Administrator/Owner
Acme Software	Acme CloudApp v1.0		CRM					
Oracle	Oracle v11		Records Management					

## 6.5. System Inventory Approach

OSCAL makes two approaches available for depicting the system inventory:

- **Flat-File Approach:** Similar to today's FedRAMP Integrated inventory workbook, where all of the information on a spreadsheet row is captured in a single assembly.
- **Component-Based Approach:** A component is defined once with as much known detail as possible, and inventory-items point to components for common information.

**FedRAMP SSP tools must support both approaches.** FedRAMP prefers the component-based approach, but will accept the flat-file approach to aid CSPs who are converting their existing MS-Excel based FedRAMP Integrated Inventory Workbook to OSCAL.



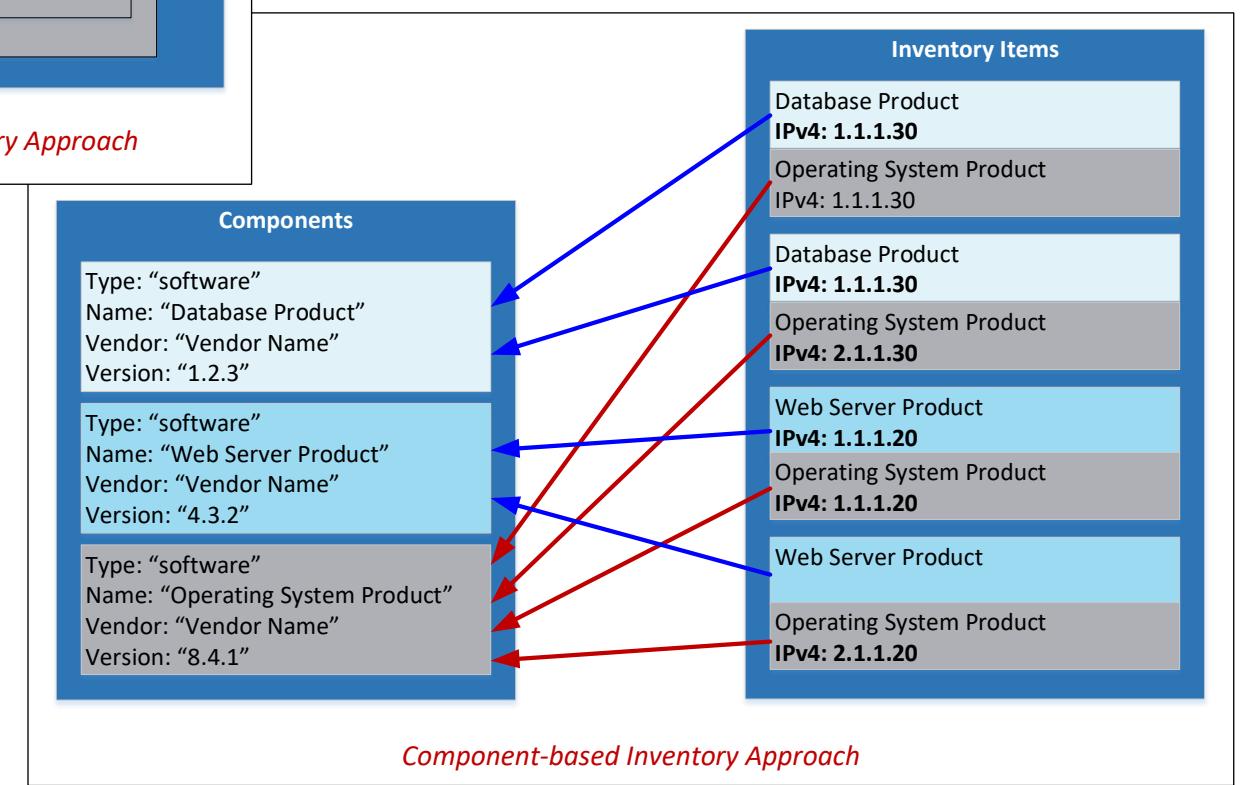
With the **flat-file approach**, all of the content on a spreadsheet row appears in a single OSCAL inventory-item assembly. The component assembly is not used. This results in a great deal of redundant information, but is a simple transition from the current spreadsheet approach.

With the **component-based approach**, common information is captured once for the component. Then each instance of that component is listed in the inventory with only the information that is unique to that component.

For example, if the same Linux operating system is used as the platform for all database and web servers, most of the details about the Linux operating system can be captured once as a component. This includes information such as vendor name, version number, and patch level.

If four Linux instances are used, each instance is an inventory item with a unique IP address and MAC address. Only those unique pieces are captured at the inventory level. All four inventory-items point back to the component for vendor name, version number, and patch level.

Initially FedRAMP will be more flexible about the CSP's inventor approach until these concepts have been applied and real-world exceptions analyzed.



## ATTACHMENT I3 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a s

The FedRAMP Inventory Workbook can be found on the following [FedRAMP website page](#). [Templates](#).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

	All Inventories			
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes
Software Example	123.45.78.400	123.45.78.400	No	No
Database Example	123.45.78.401	123.45.78.401	No	No

### NIST Accepted Values

- ```
prop
  • name="virtual"
    ○ Valid: yes, no
  • name="public"
    ○ Valid: yes, no
annotation
  • name="allows-authenticated-scan"
    ○ Valid: yes, no
  • name="is-scanned"
    ○ Valid: yes, no
```

| OS/Infrastructure Inventory | | | | | | | | |
|-----------------------------|----------------|--------------------|-----------------------------|---------------------|----------|------------|---------------------|----------------|
| NetBIOS Name | MAC Address | Authenticated Scan | Baseline Configuration Name | OS Name and Version | Location | Asset Type | Hardware Make/Model | In Latest Scan |
| linux01 | 00:00:00:00:00 | Yes | Base Config1 | Cent | | | | |

FedRAMP Accepted Values

- ```
prop
 • name="asset-type"
 ○ Valid: os, database, web-server, dns-server, email-server, directory-server, pbx, firewall, router, switch, storage-array
Other values are allowed for now.
```

Software and Database Inventories			Any Inventory					
Software Vendor	Software Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Acme Software	Acme CloudApp v1.0	CPM4						
Oracle								

The description and remarks fields are *Markup multiline*, which enables the text to be formatted.

This requires special handling. See Section 2.5.3 *Markup-line* and *Markup-multiline* Fields in OSCAL, or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

### 6.5.1. Flat File Approach

#### Flat-File Representation

```
<!-- cut -->
<system-implementation>
 <!-- interconnection -->
 <system-inventory>
 <inventory-item id="inv-1" asset-id="unique-asset-id">
 <description><p>Flat-File Example (No implemented-component).</p></description>
 <prop name="ipv4-address">0.0.0.0</prop>
 <prop name="ipv6-address">0000:0000:0000:0000</prop>
 <prop name="virtual">no</prop>
 <prop name="public">no</prop>
 <prop name="fqdn">dns.name</prop>
 <prop name="uri">uniform.resource.identifier</prop>
 <prop name="netbios-name">netbios-name</prop>
 <prop name="mac-address">00:00:00:00:00</prop>
 <prop name="software-name">software-name</prop>
 <prop name="version">V 0.0.0</prop>
 <prop name="asset-type">os</prop>
 <prop name="vendor-name" ns="https://fedramp.gov/ns/oscal">Vendor Name</prop>
 <prop name="model">Model Number</prop>
 <prop name="patch-level">Patch-Level</prop>
 <prop name="serial-number">Serial #</prop>
 <prop name="asset-tag">Asset Tag</prop>
 <prop name="vlan-id">VLAN Identifier</prop>
 <prop name="network-id">Network Identifier</prop>
 <prop name="scan-type" ns="https://fedramp.gov/ns/oscal">infrastructure</prop>
 <prop name="validation" ns="https://fedramp.gov/ns/oscal">component-id</prop>
 <annotation name="allows-authenticated-scan" value="no">
 <remarks><p>If no, explain why. If yes, omit remarks field.</p></remarks>
 </annotation>
 <annotation name="baseline-configuration-name" value="Baseline Config. Name" />
 <annotation name="physical-location" value="Physical location of Asset" />
 <annotation name="is-scanned" value="yes">
 <remarks><p>If no, explain why. If yes, omit remarks field.</p></remarks>
 </annotation>
 <annotation name="function" value="Required brief, text-based description.">
 <remarks><p>Optional, longer, formatted description.</p></remarks>
 </annotation>
 <responsible-party role-id="asset-owner">
 <party-id>person-7</party-id>
 </responsible-party>
 <responsible-party role-id="asset-administrator">
 <party-id>it-dept</party-id>
 </responsible-party>
 <implemented-component component-id="comp-router-1" />
 <remarks><p>COMMENTS: Additional information about this item.</p></remarks>
 </inventory-item>
 <!-- Repeat the inventory-item assembly for each item in the inventory -->
</system-inventory>
<!-- system-implementation remarks -->
</system-implementation>
```

#### NIST-Defined Identifier

Required Role ID:

- asset-owner
- asset-administrator

#### XPath Queries

See Section 6.5.3, *Inventory Data Locations and XPath Queries*

#### NOTES:

system administrator and application administrator are handled the same. The value of asset-type determines whether the identified asset-administrator is managing a system or application.

## ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a s

### FedRAMP Extensions & Accepted Values

```
prop (ns="https://fedramp.gov/ns/oscal"):
 • name="vendor-name"
 • name="scan-type"
 ○ Valid: infrastructure, web, database
 • name="validation"
```

The FedRAMP Inventory Workbook can be found on the following [FedRAMP website page](#). [Templates](#).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

	All Inventories			
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	VIRTUAL	PUBLIC
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes
Software Example	123.45.78.400	123.45.78.400	No	No
Database Example	123.45.78.401	123.45.78.401	No	No

### NIST Accepted Values

```
prop
 • name="virtual"
 ○ Valid: yes, no
 • name="public"
 ○ Valid: yes, no
annotation
 • name="allows-authenticated-scan"
 ○ Valid: yes, no
 • name="is-scanned"
 ○ Valid: yes, no
```

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00	Yes	Base Config1	Cent				

### FedRAMP Accepted Values

```
prop
 • name="asset-type"
 ○ Valid: os, database, web-server, dns-server, email-server, directory-server, pbx, firewall, router, switch, storage-array
```

Other values are allowed for now.

Software and Database Inventories				Any Inventory				
Software / Database Vendor	Software / Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN / Network ID	System Administrator / Owner	Application Administrator / Owner
Arma Software	Arma Cloud Appliance	CPM						

The description and remarks fields are *Markup multiline*, which enables the text to be formatted.

This requires special handling. See [Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL](#), or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

## 6.5.2. Component-based Approach

### Component-based Representation

```
<!-- cut -->
<system-implementation>
 <component id="component-sample">
 <prop name="virtual">no</prop>
 <prop name="software-name">software-name</prop>
 <prop name="version">V 0.0.0</prop>
 <prop name="asset-type">os</prop>
 <prop name="vendor-name" ns="https://fedramp.gov/ns/oscal">Vendor Name</prop>
 <prop name="model">Model Number</prop>
 <prop name="patch-level">Patch-Level</prop>
 <prop name="scan-type" ns="https://fedramp.gov/ns/oscal">infrastructure</prop>
 <prop name="validation" ns="https://fedramp.gov/ns/oscal">component-id</prop>
 <annotation name="allows-authenticated-scan" value="no">
 <remarks><p>If no, explain why. If yes, omit remarks field.</p></remarks>
 </annotation>
 <annotation name="baseline-configuration-name" value="Baseline Config. Name" />
 <annotation name="function" value="Required brief, text-based description.">
 <remarks><p>Optional, longer, formatted description.</p></remarks>
 </annotation>
 <responsible-party role-id="asset-owner">
 <party-id>person-7</party-id>
 </responsible-party>
 <responsible-party role-id="asset-administrator">
 <party-id>it-dept</party-id>
 </responsible-party>
 </component>
 <!-- service, interconnection -->
 <system-inventory>
 <inventory-item id="inv-2" asset-id="unique-asset-id">
 <description><p>If needed, describe this instance.</p></description>
 <prop name="ipv4-address">0.0.0.0</prop>
 <prop name="public">no</prop>
 <prop name="fqdn">dns.name</prop>
 <prop name="uri">uniform.resource.identifier</prop>
 <prop name="mac-address">00:00:00:00:00:00</prop>
 <prop name="serial-number">Serial #</prop>
 <prop name="vlan-id">VLAN Identifier</prop>
 <prop name="network-id">Network Identifier</prop>
 <annotation name="is-scanned" value="yes" />
 <implemented-component component-id="component-sample" />
 <remarks><p>COMMENTS: Additional information about this item.</p></remarks>
 </inventory-item>
 <!-- Repeat the inventory-item assembly for each use of the above component -->
 </system-inventory>
 <!-- system-implementation remarks -->
</system-implementation>
```

### NIST-Defined Identifier

Required Role ID:

- asset-owner
- asset-administrator

### XPath Queries

See [Section 6.5.3, Inventory Data Locations and XPath Queries](#)

### NOTES:

- If component-sample is an image of a Linux virtual machine (VM), and 10 instances of that VM are in use, there would be one (1) component assembly and ten (10) inventory-item assemblies, all referencing the same component.

### 6.5.3. Inventory Data Locations and XPath Queries

The

		<b>Guidance</b>	<b>Valid Values</b>	<b>Requirement</b>	<b>Component</b>	<b>Inventory-Item</b>	<b>OSCAL Cardinality</b>	<b>Data Location: XPath Notation (CASE SENSITIVE)</b>	<b>NOTES</b>
<b>All Inventories</b>	<b>UNIQUE ASSET IDENTIFIER</b>	Unique Identifier associated with the asset. This Identifier should be used consistently across all documents, 3PAOs artifacts, and any vulnerability scanning tools. For OS/Infrastructure and Web Application Software, this is typically an IP address or URL/DNS name. For a database, it is typically an IP address, URL, or database name. A CSP's own naming scheme is also acceptable as long as it has unique identifiers.	Must be unique.	<u>Mandatory</u> for all inventory records.		X	1	<code>/*/system-implementation/system-inventory/inventory-item[@asset-id="___"]</code>	The system-specific "Unique Asset Identifier" must be set as the asset-id flag on the inventory-item field.
	<b>IPv4 or IPv6 Address</b>	If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column.  If a device has multiple IP addresses, then include one row in this inventory for each IP address.		Optional, unless used as Identifier in vulnerability scans or security assessments.		X	0 - ∞	<code>/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv4-address"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv6-address"]</code>	One prop field per IP address, if more than one.
	<b>Virtual</b>	Is this asset virtual?	Yes or No.	<u>Mandatory</u> for OS/Infrastructure, Software, and Database.	X	X	1	<code>/*/system-implementation/component/prop[@name="virtual"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="virtual"]</code>	Must have "Virtual" at the inventory item-level either explicitly, or via a linked component.  May define it at component level and propagate to inventory-item.
	<b>Public</b>	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	Yes or No.	<u>Mandatory</u> for OS/Infrastructure, Software, and Database.		X	1	<code>/*/system-implementation/system-inventory/inventory-item/prop[@name="public"]</code>	
	<b>DNS Name or URL</b>	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	Valid DNS name or URL.	Optional, unless used as Identifier in vulnerability scans or security assessments.		X	0 - ∞	<code>/*/system-implementation/system-inventory/inventory-item/prop[@name="fqdn"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="uri"]</code>	May use either DNS name, URL or both. Use a separate prop field for each DNS name and/or URL.

	Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
OS/Infrastructure Inventory	<b>NetBIOS Name</b>	If available, state the NetBIOS name. May be left blank if one does not exist, or dynamic.	Valid NetBIOS name.	Optional, unless used as identifier in scans or security assessments.	X	0 - $\infty$	<code>/*/system-implementation/system-inventory/inventory-item/prop[@name="netbios-name"]</code>	One prop field per NetBIOS name, if more than one.
	<b>MAC Address</b>	If available, state the MAC Address. May be left blank if one does not exist, or dynamic.	Valid MAC Address.	Optional, unless used as identifier in scans or security assessments.	X	0 - $\infty$	<code>/*/system-implementation/system-inventory/inventory-item/prop[@name="mac-address"]</code>	One prop field per MAC address, if more than one.
	<b>Authenticated Scan</b>	Is the asset is planned for an authenticated scan?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1  <code>/*/system-implementation/component/annotation[@name="allows-authenticated-scan"]/@value=""</code>  <code>/*/system-implementation/system-inventory/inventory-item/annotation[@name="allows-authenticated-scan"]/@value=""</code>	Must have "Authenticated-Scan" at the inventory-item level either explicitly or via a linked component.  May define it at component level and propagate to inventory-item.
	<b>Baseline Configuration Name</b>	If available, provide the name of the configuration template used within the CSP configuration management.	.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1  <code>/*/system-implementation/component/annotation[@name="baseline-configuration-name"]/@value=""</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="baseline-configuration-name"]/@value=""</code>	Must have "Baseline Configuration Name" at the inventory-item level either explicitly or via a linked component.  May define it at component level and propagate to inventory-item.
	<b>OS Name and Version</b>	Operating System Name and Version running on the asset.		Optional for OS/Infrastructure. Leave blank for Software and Database.	X	0 or 1	<code>/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]</code>  <code>/*/system-implementation/component/prop[@name="version"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]</code>	Use software name and version, and set asset-type of "os". Required for operating systems.  Must have "OS Name and Version" at the inventory-item level either explicitly or via a linked component. May define it at the component level and propagate to inventory item.
	<b>Location</b>	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	Valid locations for CSP infrastructure.	Optional for OS/Infrastructure. Leave blank for Software and Database.	X	0 or 1	<code>/*/system-implementation/system-inventory/inventory-item/prop[@name="physical-location"]/@value=""</code>	
	<b>Asset Type</b>	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1  <code>/*/system-implementation/component/prop[@name="asset-type"]</code>  <code>/*/system-implementation/system-inventory/inventory-item[@name="asset-type"]</code>	Must use an Accepted Value (see Registry) if an applicable one exists.  Must have "Asset Type" at the inventory-item level, either explicitly or via a linked component. May define it at component level and propagate to inventory-item.
	<b>Hardware Make/Model</b>	Name of the hardware product and model.		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	0 or 1  <code>/*/system-implementation/component/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]</code>  <code>/*/system-implementation/component/prop[@name="model"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]</code>  <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="hardware-model"]</code>	Must have "Hardware Vendor" and "Hardware Model" at the inventory item-level either explicitly, or via a linked component. May define it at component level and propagate to inventory-item.  <b>NOTE:</b> @name="model" at component level, but @name="hardware-model" at inventory level.
	<b>In Latest Scan</b>	Should the asset appear in the network scans and can it be probed by the scans creating the current POA&M?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	1	<code>/*/system-implementation/system-inventory/inventory-item/annotation[@name="is-scanned"]/@value=""</code>	

	<b>Guidance</b>	<b>Valid Values</b>	<b>Requirement</b>	<b>Component</b>	<b>Inventory-Item</b>	<b>OSCAL Cardinality</b>	<b>Data Location: XPath Notation (CASE SENSITIVE)</b>	<b>NOTES</b>
<b>Software and Database Inventories</b>	<b>Software/Database Vendor</b>	Name of Software or Database vendor.	If open source (e.g., there is no "vendor"), enter "Open Source" as the vendor name.	Mandatory for Software and Database. Leave blank for OS/Infrastructure.	X	X	<b>0 or 1</b>	<pre>/*/system-implementation/component/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]</pre> <pre>/*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]</pre>
	<b>Software/Database Name &amp; Version</b>	Name of Software or Database product and version number.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	X	<b>0 or 1</b>	<pre>/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]</pre> <pre>/*/system-implementation/component/prop[@name="version"]</pre> <pre>/*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]</pre> <pre>/*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]</pre>
	<b>Patch Level</b>	If applicable.	Optional if applicable. Otherwise, leave blank.	X	X	<b>0 or 1</b>	<pre>/*/system-implementation/component/prop[@name="patch-level"]</pre> <pre>/*/system-implementation/system-inventory/inventory-item/prop[@name="software-patch-level"]</pre>	The "Patch Level" may be specified at the component or inventory-item level.
	<b>Function</b>	For Software or Database, the function provided by the Software or Database for the system.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	X	<b>0 or 1</b>	<pre>/*/system-implementation/component/annotation[@name="function"]/@value=""</pre> <pre>/*/system-implementation/component/annotation[@name="function"]/remarks</pre> <pre>/*/system-implementation/system-inventory/inventory-item/annotation[@name="function"]/@value=""</pre> <pre>/*/system-implementation/system-inventory/inventory-item/annotation[@name="function"]/remarks</pre>

	Guidance	Valid Values	Requirement	Component	Inventory -Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
Any Inventory	Comments	Any additional information that could be useful to the reviewer.		Optional for OS/Infrastructure, Software and Database.	X	X	<b>0 or 1</b> <code>/*/system-implementation/component/remarks</code> <code>/*/system-implementation/system-inventory/inventory-item/remarks</code>	May have comments in either the component level, inventory-item level or both.
	Serial #/Asset Tag#	Product serial number or internal asset tag #.		Optional for OS/Infrastructure, Software, and Database.		X	<b>0 or 1</b> <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="serial-number"]</code> <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="asset-tag"]</code>	
	VLAN/Network ID	Virtual LAN or Network ID.		Optional for OS/Infrastructure, Software, and Database.		X	<b>0 or 1</b> <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="vlan-id"]</code> <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="network-id"]</code>	
	System Administrator or/ Owner	Name of the system administrator or owner.		Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	X	X	<b>1</b> <code>COMPONENT OWNER (Person):</code> <code>/*/metadata/party[@id=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-id]/person/person-name</code> <code>COMPONENT ADMINISTRATOR (Org):</code> <code>/*/metadata/party[@id=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-id]/org/org-name</code> <code>INVENTORY ITEM OWNER (Person):</code> <code>/*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-id]/person/person-name</code> <code>INVENTORY ITEM ADMINISTRATOR (Org):</code> <code>/*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-id]/org/org-name</code>	Must have "System Owner/Administrator" at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "system owner/administrator" at the component level.
	Application Administrator or/ Owner	Name of the application administrator or owner.		Optional for OS/Infrastructure, Software, and Database.	X	X	<b>1</b> <code>COMPONENT OWNER (Person):</code> <code>/*/metadata/party[@id=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-id]/person/person-name</code> <code>COMPONENT ADMINISTRATOR (Org):</code> <code>/*/metadata/party[@id=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-id]/org/org-name</code> <code>INVENTORY ITEM OWNER (Person):</code> <code>/*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-id]/person/person-name</code> <code>INVENTORY ITEM ADMINISTRATOR (Org):</code> <code>/*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-id]/org/org-name</code>	Must have "Application Owner/Administrator" at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "system owner/administrator" at the component level.
	Scan Type	Indicate which scan type(s) the item is subjected to.	infrastructure , database, web-server	Mandatory	X	X	<b>1</b> <code>/*/system-implementation/component/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]</code> <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]</code>	Valid values: infrastructure, web, database. If more than one type is applicable, use one field per type.
ADDITIONAL	FIPS 140-2 Validation	Indicate the certificate information for an inventory item with a FIPS 140-2 validated cryptographic module.	component-id	Mandatory for any item involving cryptography. Omit otherwise.	X	X	<b>0 - ∞</b> <code>/*/system-implementation/component/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]</code> <code>/*/system-implementation/system-inventory/inventory-item/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]</code>	If an item has more than one cryptographic module, use one entry per validation certificate. May define "FIPS 140-2 validation" at the component level and propagate to the inventory-item level.

## ATTACHMENT I3 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](#).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory									
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan	
linux01	00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No	

Software and Database Inventories				Any Inventory					
Software/Database Vendor	Software/Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/Network ID	System Administrator/Owner	Application Administrator/Owner	
Acme Software	Acme CloudApp v1.0		CRM						
Oracle	Oracle v11		Records Management						

### XPath Queries

Number of Inventory Items:  
`count(//*[@system-implementation/system-inventory/inventory-item])`

Number of Hardware Components:  
`count(//*[@system-implementation/component[@component-type="hardware"]])`

Number of Software Components:  
`count(//*[@system-implementation/component[@component-type="software"]])`

In Latest Scan?:  
`//*[@system-implementation/system-inventory/inventory-item[1]/annotation[@name="is-scanned"]]/@value`

Replace "[1]" with "[2]", "[3]", etc.

List Inventory Items Not Scanned:  
`//*[@system-implementation/system-inventory/inventory-item/annotation[@name="is-scanned"][@value='no']]//prop[@name='ipv4-address']`

List of Reasons Inventory Items Were Not Scanned:  
`//*[@system-implementation/system-inventory/inventory-item/annotation[@name="is-scanned"][@value='no']]//remarks`

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See [Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL](#), or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

## ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](#).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

All Inventories			
IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column.  If a device has multiple IP addresses, then include one row in this inventory for each IP address.	Is this asset virtual?  Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.		If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.
	Yes or No.	Yes or No.	Valid DNS name or URL.
<small>Optional, unless used as identifier in vulnerability scans or security assessments.</small>	<small>Mandatory for OS/Infrastructure, Software, and Database.</small>	<small>Mandatory for OS/Infrastructure, Software, and Database.</small>	<small>Optional, unless used as identifier in vulnerability scans or security assessments.</small>

Any Inventory				
Comments	Serial#/Asset Tag#	VLAN/Network ID	System Administrator/Owner	Application Administrator/Owner
Any additional information that could be useful to the reviewer.	Product serial number or internal asset tag #.	Virtual LAN or Network ID.	Name of the system administrator or owner.	Name of the application administrator or owner.
<small>Optional for OS/Infrastructure, Software and Database.</small>	<small>Optional for OS/Infrastructure, Software, and Database.</small>	<small>Optional for OS/Infrastructure, Software, and Database.</small>	<small>Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.</small>	<small>Optional for OS/Infrastructure, Software, and Database.</small>

Unlike most XPath 2.0 queries in this document, the following queries cannot be easily converted to XPath 1.0 . If working with XPath 1.0, it may be necessary to perform each search with two queries. These queries will list all the IPv4 addresses for each scan type (infrastructure, web, and database), whether using the flat-file inventory approach or the component-based approach.

### XPath 2.0 Queries

IPv4 Address of All Inventory Items Identified for **Infrastructure Scanning**:

```
distinct-values((let $key:=/*/system-implementation/component[prop[@name='scan-type']]@ns='https://fedramp.gov/ns/oscal'][@name='infrastructure'])/@id return /*/system-implementation/system-inventory/inventory-item [implemented-component/@component-id=$key]/prop[@name='ipv4-address']) | /*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-address'][..]/prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal'][string(.)='infrastructure']))
```

IPv4 Address of All Inventory Items Identified for **Web Scanning**:

```
distinct-values((let $key:=/*/system-implementation/component[prop[@name='scan-type']]@ns='https://fedramp.gov/ns/oscal'][@name='web'])/@id return /*/system-implementation/system-inventory/inventory-item [implemented-component/@component-id=$key]/prop[@name='ipv4-address']) | /*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-address'][..]/prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal'][string(.)='web']))
```

IPv4 Address of All Inventory Items Identified for **Database Scanning**:

```
distinct-values((let $key:=/*/system-implementation/component[prop[@name='scan-type']]@ns='https://fedramp.gov/ns/oscal'][@name='database'])/@id return /*/system-implementation/system-inventory/inventory-item [implemented-component/@component-id=$key]/prop[@name='ipv4-address']) | /*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-address'][..]/prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal'][string(.)='database']))
```

Items Where an Authenticated Scan is Possible:

```
distinct-values(/*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-address'][..]/annotation[@name='allows-authenticated-scan'][@value='yes']]) | (let $key:=/*/system-implementation/component[annotation[@name='allows-authenticated-scan'][@value='yes']]@id return /*/system-implementation/system-inventory/inventory-item [implemented-component/@component-id=$key]/prop[@name='ipv4-address']))
```

Items Where an Authenticated Scan is Not Possible:

```
distinct-values(/*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-address'][..]/annotation[@name='allows-authenticated-scan'][@value='no']]) | (let $key:=/*/system-implementation/component[annotation[@name='allows-authenticated-scan'][@value='no']]@id return /*/system-implementation/system-inventory/inventory-item [implemented-component/@component-id=$key]/prop[@name='ipv4-address']))
```

Authenticated Scan Justification (if Authenticate Scan is "no"):

```
/*/system-implementation/system-inventory/inventory-item/annotation[@name='allows-authenticated-scan'][@value="no"])/remarks
```

OR

```
/*/system-implementation/component/annotation[@name='allows-authenticated-scan'][@value="no"])/remarks
```

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See [Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL](#), or visit: <https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline>

## 7. GENERATED CONTENT

The following artifacts are historically generated by hand to summarize content found in other portions of the FedRAMP SSP. When using OSCAL, these artifacts can be generated from content found elsewhere in this document. This includes the:

- **Control Information Summary (CIS)**
- **Customer Responsibility Matrix (CRM)**

If delivering SSP content in OSCAL, CSPs are no longer required to manually generate and maintain these artifacts, provided the content in their OSCAL-based FedRAMP SSP remains accurate.

**Tool developers are encouraged to develop their own solutions to generating this content.**

### 7.1. Generating the Control Information Summary (CIS)

There are many ways a tool developer can generate the CIS. FedRAMP is developing an Extensible Stylesheet Language Transformation (XSLT) file to generate the FedRAMP CIS. When ready, FedRAMP will make this freely available to the public here:

<https://github.com/GSA/fedramp-automation/tree/master/resources>

### 7.2. Generating the Customer Responsibility Matrix (CRM)

There are many ways a tool developer can generate the CRM. FedRAMP is developing an Extensible Stylesheet Language Transformation (XSLT) file to generate the FedRAMP CRM. When ready, FedRAMP will make this freely available to the public here:

<https://github.com/GSA/fedramp-automation/tree/master/resources>

Useful CRM XPath Queries
<pre>Flat-File CRM Query: //control-implementation/implemented-requirement/annotation[@name= "control-origination"][@ns="https://fedramp.gov/ns/oscal"] [@value="customer-configured" or @value="customer-provided"]/remarks</pre>
<pre>Component-based CRM Query: //control-implementation/implemented-requirement/statement/by-component [@component-id="customer"]/description</pre>

## APPENDICES

### APPENDIX A. OSCAL-BASED FEDRAMP BASELINES

The system's identified security categorization level governs which FedRAMP baseline applies. This can be checked using the XPath syntax below.

#### Security Sensitivity Level XPath Query

Security Categorization Level:  
`/*/system-characteristics/security-sensitivity-level`

This determines which URL should be entered for the `import-profile` field in an OSCAL-based FedRAMP SSP.

#### Baseline Representation

```
<!-- metadata -->
<!-- This must point to the appropriate FedRAMP Baseline -->
<import-profile href="https://path/to/FedRAMP_MODERATE-baseline_profile.xml"/>
<!-- system-characteristics -->
```

FedRAMP validation tools will compare the identified security categorization level to the actual FedRAMP baseline specified in the SSP and raise a warning if a different baseline was used.

#### High

##### XML Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP\\_HIGH-baseline\\_profile.xml](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_HIGH-baseline_profile.xml)

##### JSON Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP\\_HIGH-baseline\\_profile.json](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_HIGH-baseline_profile.json)

#### Moderate

##### XML Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP\\_MODERATE-baseline\\_profile.xml](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_MODERATE-baseline_profile.xml)

##### JSON Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP\\_MODERATE-baseline\\_profile.json](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_MODERATE-baseline_profile.json)

#### Low

##### XML Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP\\_LOW-baseline\\_profile.xml](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_LOW-baseline_profile.xml)

##### JSON Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP\\_LOW-baseline\\_profile.json](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_LOW-baseline_profile.json)

Do not copy and modify the FedRAMP baseline. FedRAMP will use the original, published file for validation, ignoring any modified copies.

If you require a modification to the FedRAMP baselines, such as may be required when directed to do so by an authorizing official, first contact FedRAMP to coordinate the modification, then follow the instructions in Appendix B.

## FedRAMP Tailored

FedRAMP Tailored for Low Impact – Software as a Service (LI-SaaS) Appendix B merges SSP, SAP, and SAR information into a single document. The SSP portions of that document may be represented using the same OSCAL conventions described in this document with only a few minor differences.

Fully representing Appendix B in OSCAL requires syntax that has not yet been developed. For these reasons, a separate guide will be developed for FedRAMP Tailored once the appropriate syntax has been defined.

For your convenience, FedRAMP has made the FedRAMP Tailored for LI-SaaS baseline available now in both XML and JSON formats as follows:

### Low-Impact SaaS (Tailored)

#### XML Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/  
FedRAMP\\_LI-SaaS-baseline\\_profile.xml](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_LI-SaaS-baseline_profile.xml)

#### JSON Version:

[https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/  
FedRAMP\\_LI-SaaS-baseline\\_profile.json](https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_LI-SaaS-baseline_profile.json)

## APPENDIX B. MODIFYING A FEDRAMP BASELINE

OSCAL is designed to allow modification of controls and baselines, while maintaining traceability through each layer of modification. This means you should never copy and modify a FedRAMP baseline.

If you require a change to a FedRAMP baseline, you should first coordinate that change with the FedRAMP JAB or PMO. Assuming FedRAMP agrees with the change, the correct way to implement the change is as follows:

1. **Create a new, blank OSCAL Profile.**
2. **Point to the FedRAMP Baseline:** Point it to the appropriate FedRAMP baseline using an `import` field.
3. **Select the Relevant Controls:** Use the `include` and `exclude` fields to identify the controls to include or exclude from the FedRAMP baseline.
  - a. For example, if you need all but one control, you can `include all`, then `exclude` the one.
4. **Specify How Controls Are Organized:** FedRAMP prefers you merge "as-is" using those merge fields. This is relevant when resolving the profile. See the *Profile Resolution* section of this appendix for more information.
5. **Modify the Selected Controls:** Use the `modify` assembly to make modifications to parameters and control definitions.

The next page contains an example profile, which accomplishes the following actions:

- Imports the FedRAMP Moderate baseline
- Includes all controls from that baseline
- Explicitly removes AT-4 from the baseline
- Indicates that if this profile is resolved the organization of the controls should remain as-is. See the *Profile Resolution* section of this appendix for more information.
- Adds a constraint to the third parameter of AC-1 (ac-1\_prm\_3), which is more restrictive than the FedRAMP constraint, but changing it from "at least annually" to "at least every six months".
- Removes the additional FedRAMP requirement statement in AU-11 and replaces it with a more restrictive statement, which now requires online retention of audit records for at least 180 days instead of 90 days.

For more information on working with profiles, please visit the NIST OSCAL site at:

<https://pages.nist.gov/OSCAL>

A complete OSCAL profile syntax reference is available here:

<https://pages.nist.gov/OSCAL/documentation/schema/profile/>

**Sample Profile to Modify a FedRAMP Baseline**

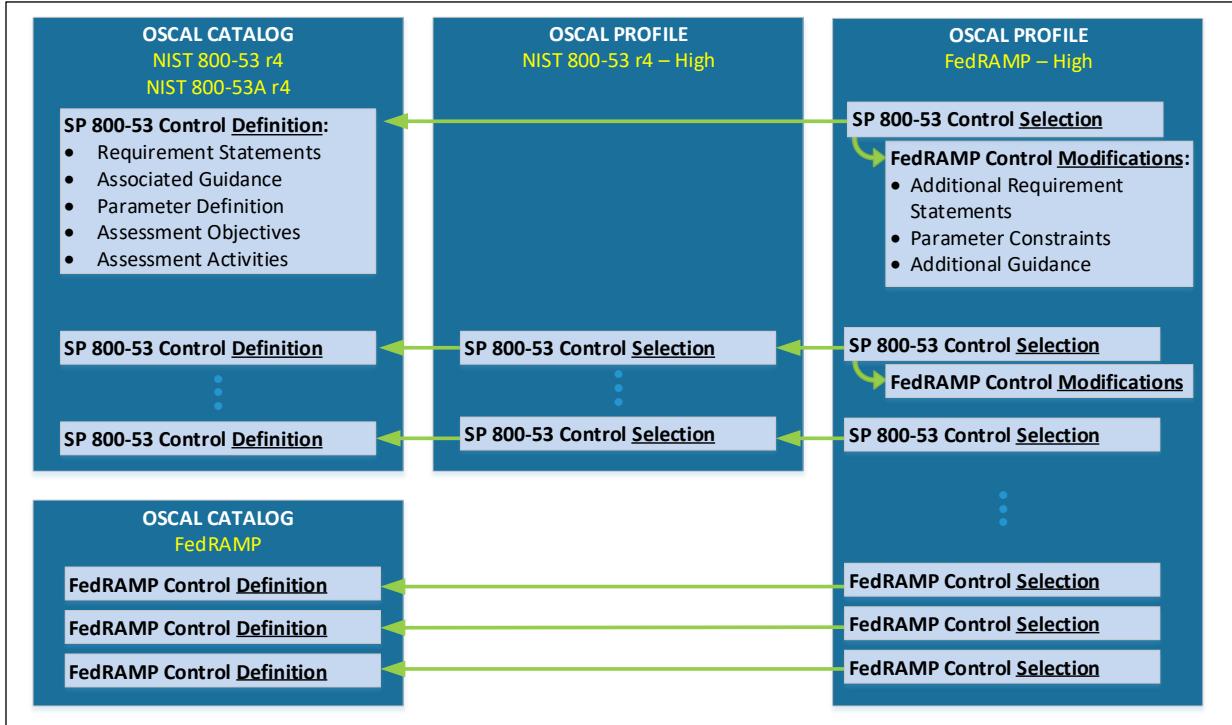
```

<profile xmlns="http://csrc.nist.gov/ns/oscal/1.0"
 id="uuid-xxxx">
 <metadata>
 <title>[XYZ Org] Modification to FedRAMP Moderate
Baseline</title>
 <last-modified>2019-10-01T11:03:27.392-04:00</last-modified>
 <version>1.1</version>
 <oscal-version>1.0.0-milestone2</oscal-version>
 </metadata>
 <import href="https://path/to/FedRAMP_MODERATE-baseline_profile.xml">
 <include>
 <!-- Include every control in the Moderate baseline -->
 <all with-child-controls="yes" />
 </include>
 <exclude>
 <!-- Remove Control AT-4 -->
 <call control-id="at-4" />
 </exclude>
 </import>
 <merge><as-is>yes</as-is></merge>
 <modify>
 <set param-id="ac-1_prm_3">
 <!-- Change the constraint from "at least annually" -->
 <constraint>at least every six months</constraint>
 </set>
 <remove id-ref="au-11_fr" />
 <alter control-id="au-11">
 <add position="ending">
 <part id="au-11_fr" name="item"
ns="https://fedramp.gov/ns/oscal">
 <title>[XYZ Org] Modified Requirement</title>
 <part id="au-11_fr_smt.1" name="item">
 <prop name="label">Requirement:</prop>
 <p>The service provider retains audit
records on-line for at 180 days and further preserves audit records off-line
for a period that is in accordance with NARA requirements.</p>
 </part>
 </part>
 </add>
 </alter>
 </modify>
</profile>

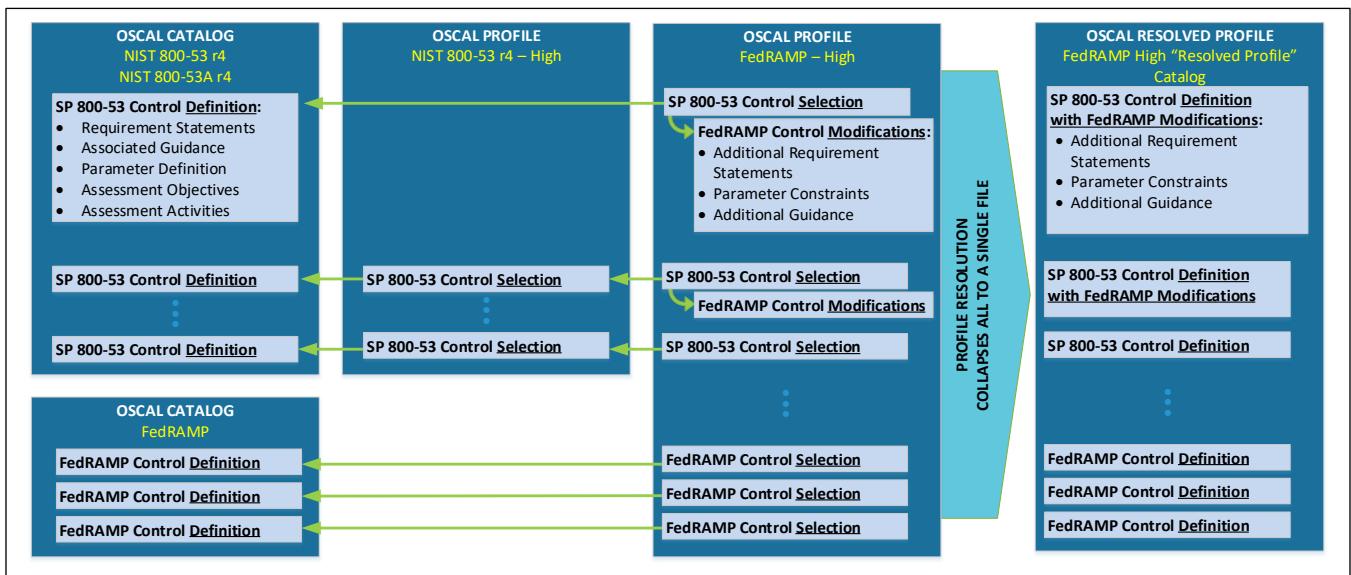
```

## Profile Resolution

Profiles are intended to identify upstream sources of control definition information and show only the changes to those upstream sources. This enables humans and computers to trace control definition changes back to their source framework.



An organization may prefer to work with a single, complete file containing only the final set of relevant control definitions. OSCAL provides a process for merging this collection of catalogs and profiles into a single catalog. This process is called "profile resolution".



The `merge` assembly within an OSCAL profile offers a profile creator control over how the final file is organized. To maintain the same organization, simply use the `as-is` field and set it to "yes".

The complete profile syntax is available here:

<https://pages.nist.gov/OSCAL/documentation/schema/profile/>

## APPENDIX C. WORKING WITH ROLES, PEOPLE, AND ORGANIZATIONS

An OSCAL SSP file defines roles, people, and organizations within the metadata as part of three separate assemblies:

- **role**: A role ID and role title are required. Other content, such as a short-name, description, or remarks are optional.
- **party**: People and organizations are defined next as parties. An organization is any collection of people, and can represent a company, agency, department, or team.
- **responsible-party**: Links roles to parties. The same role can have more than one party assigned to it. Also a party can be assigned to more than one role.

### Working with Role Identifiers

All roles within the document are defined under the metadata element as follows:

```
<metadata>
 --- cut ---
 <role id="prepared-by">
 <title>Prepared By</title>
 <desc>The organization that prepared this SSP.</desc>
 </role>
 <role id="prepared-for">
 <title>Prepared For</title>
 <desc>The organization for which this SSP was prepared</desc>
 </role>
 --- cut ---
</metadata>
```

To ensure consistent processing, FedRAMP has defined a specific set of roles that must exist with a FedRAMP SSP with the provided role identifiers. **Most are pre-populated in the OSCAL-based FedRAMP SSP Template.** CSPs must ensure these roles, titles, and descriptions exist within an OSCAL-based FedRAMP SSP. CSPs may add additional roles, provided these roles remain.

**NIST-defined and FedRAMP-defined role-identifiers are cited in relevant portions of this document, and summarized in the FedRAMP OSCAL Registry.**

### FedRAMP Defined Party Identifiers

To ensure consistent processing, FedRAMP has defined a specific set of party identifiers that must exist with a FedRAMP SSP with the provided party identifiers. **Some are pre-populated in the OSCAL-based FedRAMP SSP Template.** CSPs must ensure these party identifiers are used where appropriate. CSPs may assign their own details to these parties; however, FedRAMP's systems will search for the defined party using these IDs.

**FedRAMP-defined party identifiers are cited in relevant portions of this document, and summarized in the FedRAMP OSCAL Registry.**

## APPENDIX D. WORKING WITH COMPONENTS

NIST designed OSCAL such that a system architect can express all aspects of the system as components. A component is anything that can satisfy a control requirement. This includes hardware, software, services, and underlying service providers, as well as policies, plans, and procedures. There are several ways to use components in an OSCAL-based SSP. The following defines FedRAMP's minimum initial use.

*Anything that can satisfy a control requirement is a component, including hardware, software, services, policies, plans, and procedures.*

This section will likely be updated as NIST continues to evolve its approach to components in OSCAL, and as FedRAMP receives feedback from stakeholders.

**FedRAMP-defined component identifiers are cited in relevant portions of this document, and summarized in the FedRAMP OSCAL Registry.**

### Minimum Required Components

There must be a component that represents the entire system itself, and has the ID "system".

If there is one or more controls with a `customer-provided` or `customer-configured` control origination, there should also be a component that represents customers and has the ID "customer". The implementation statements are tied to this component as described in *Section 5.6, Control Implementation Description: Approaches*, and are summarized into the Customer Responsibility Matrix (CRM).

The following is an example of defined components.

#### Minimum Required Component Representation

```
<!-- system-characteristics -->
<system-implementation>
 <!-- user -->

 <!-- This System -->
 <component id="system" name="This System" component-type="system" >
 <description><p>
 The entire system as depicted in the system authorization boundary.
 </p></description>
 <status state="operational" />
 </component>

 <!-- Customer -->
 <component id="customer" name="Customer" component-type="customer" >
 <description><p>Customer's Responsibility</p></description>
 <status state="other" />
 </component>
</system-implementation>
```

## Common Additional Components

If there is an underlying FedRAMP-authorized system, from which the subject system is inheriting controls, there must be a component for that as well, with the ID "comp-fedramp-authorized-provider-1".

For each FIPS 140-2 validated module, there must be a component that represents the validation certificate itself. For more information about this, see the *FIPS 140-2 Validated Components* Section.

### Common Additional Component Representation

```
<!-- system-characteristics -->
<system-implementation>
 <!-- user -->
 <!-- Minimum Required Components -->

 <!-- Leveraged FedRAMP-authorization system -->
 <component id="comp-fedramp-authorized-provider"
 name="[Provider System's Name]" component-type="service" >
 <description><p>A FedRAMP-authorized system.</p></description>
 <prop name="authorization-date" ns="https://fedramp.gov/ns/oscal">2019-01-01</prop>
 <status state="operational" />
 </component>

 <!-- FIPS 140-2 Validation Certificate Information -->
 <!-- Include a separate component for each relevant certificate -->
 <component id="comp-fips-module-1" name="Name" component-type="validation">
 <description><p>FIPS 140-2 Validated Module</p></description>
 <prop name="cert-no" ns="https://fedramp.gov/ns/oscal">0000</prop>
 <link href="https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/0000" />
 <status state="operational" />
 </component>

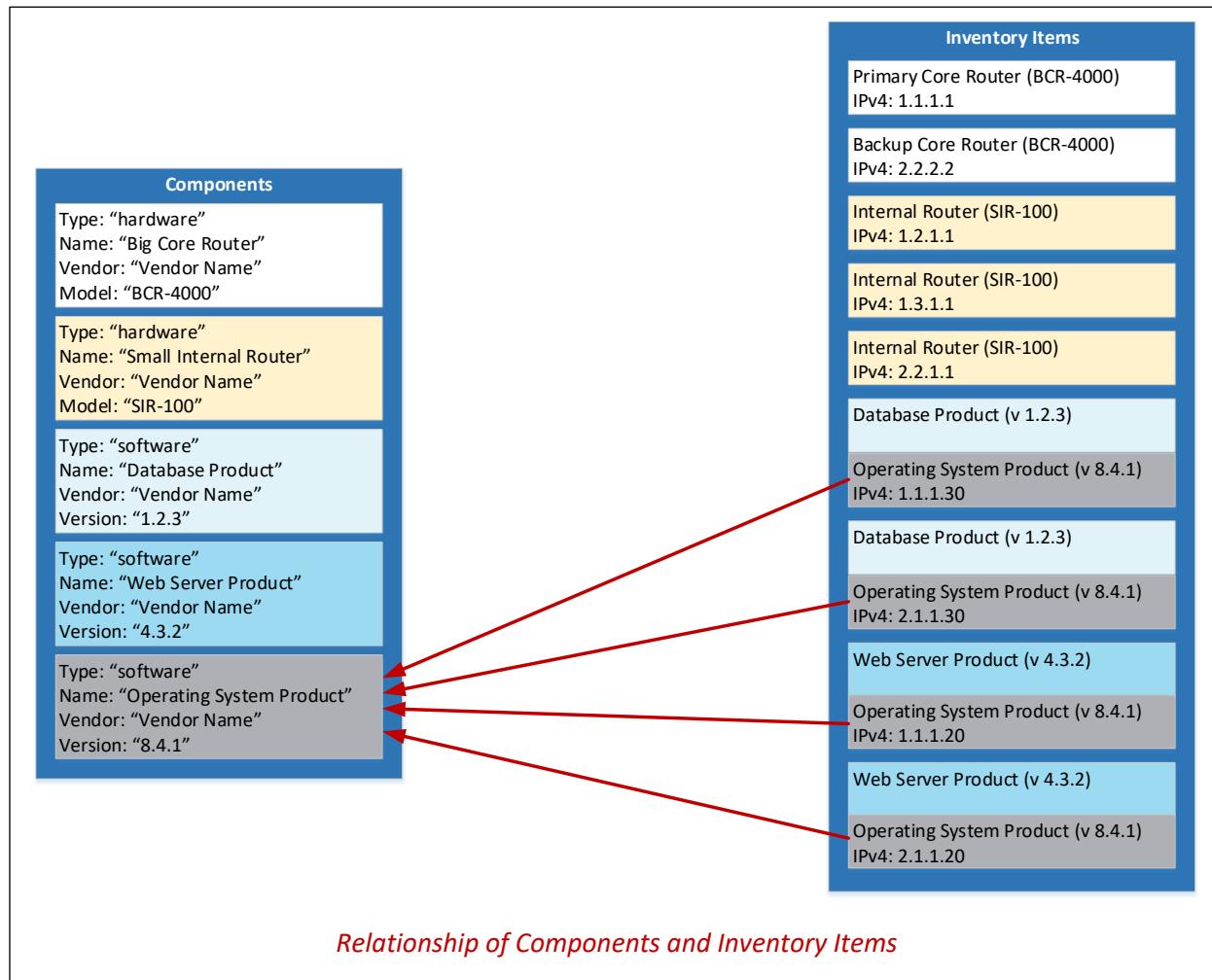
 <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

## Components as a Basis for System Inventory

NIST's approach to component-based system modeling is to reduce redundancy of information and increase flexibility. NIST accomplishes this with separate component and inventory item modeling.

This is a one-to-many relationship. One component to many inventory item instances.

For example, if an open source operating system (OS) is used in many places throughout the system, it is defined once as a component. All information about the product, vendor, and support are modeled within the component detail. If the OS is used four times within the system, each use is an inventory item, with details about that specific information, such as IP address,



FedRAMP requires a component assembly for each model of infrastructure device used, and each version of software and database used within the system. FedRAMP is not asking for more detail than provided in the legacy inventory workbook. Only that the information is organized differently.

As NIST continues to evolve its component approach, FedRAMP will re-evaluate its approach to system inventory representation.

## FIPS 140-2 Validated Components

NIST's component model treats independent validation of products and services as if that validation were a separate component. This means when using components with FIPS 140-2 validated cryptographic modules:

- **The Validation Definition:** A component definition that provides details about the validation.
- **The Product Definition:** A component definition that describes the hardware or software product.

The validation definition is a component definition that provides details about the independent validation. In the case of FIPS 140-2 validation, this must provide the certificate number, and the link to entry in the NIST Computer Security Resource Center (CSRC) [Cryptographic Module Validation Program Database](#).

In the future, NIST will provide syntax that allows the product and the validation to be linked; however, this syntax is not yet available, so FedRAMP is providing alternative syntax to accomplish the linking.

While FedRAMP requires the separate component definition for FIPS 140-2 validation, linking those components using the FedRAMP extension is optional. Once NIST provides final syntax to link a product and its validation, that link will become mandatory.

Component Representation: Example Product With FIPS 140-2 Validation
<pre>&lt;!-- system-characteristics --&gt; &lt;system-implementation&gt;     &lt;!-- user --&gt;     &lt;!-- Minimum Required Components --&gt;      &lt;!-- FIPS 140-2 Validation Certificate Information --&gt;     &lt;!-- Include a separate component for each relevant certificate --&gt;     &lt;component id="comp-fips-module-1" name="Name" component-type="validation"&gt;         &lt;description&gt;&lt;p&gt;FIPS 140-2 Validated Module&lt;/p&gt;&lt;/description&gt;         &lt;prop name="cert-no" ns="https://fedramp.gov/ns/oscal"&gt;0000&lt;/prop&gt;         &lt;link href="https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/0000" /&gt;         &lt;status state="operational" /&gt;     &lt;/component&gt;      &lt;!-- FIPS 140-2 Validated Product --&gt;     &lt;component id="comp-validated-product"                 name="Product Vendor" component-type="software" &gt;         &lt;description&gt;&lt;p&gt;A product with a cryptographic module.&lt;/p&gt;&lt;/description&gt;         &lt;status state="operational" /&gt;     &lt;/component&gt;      &lt;!-- service --&gt; &lt;/system-implementation&gt; &lt;!-- control-implementation --&gt;</pre>